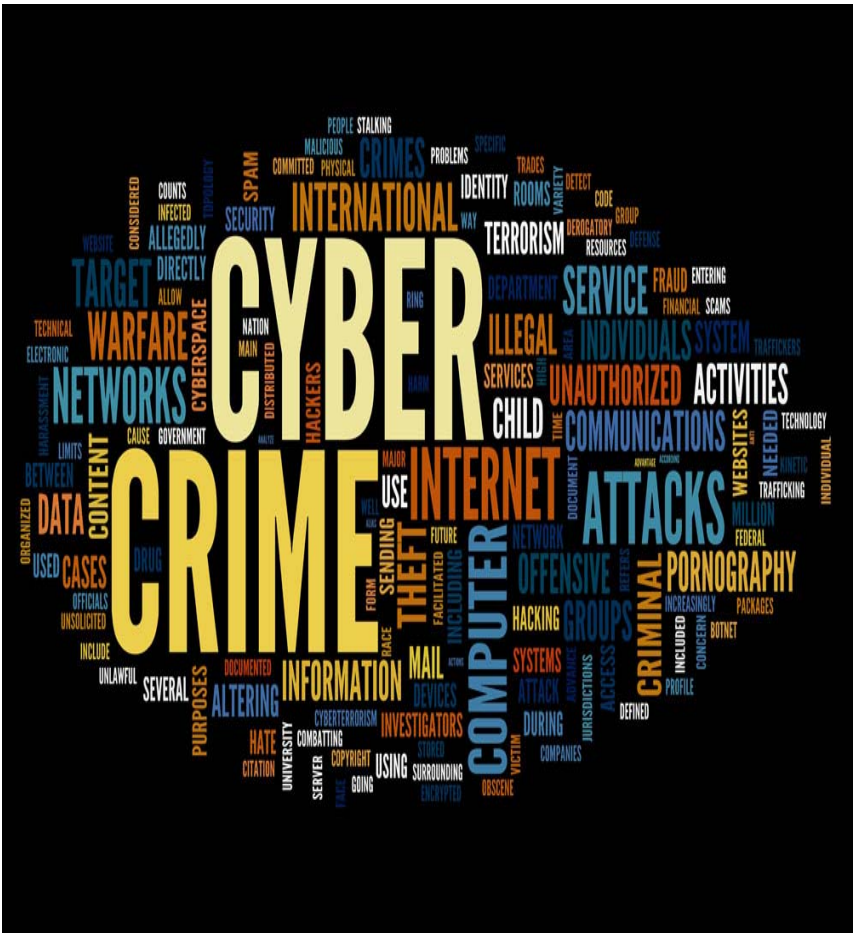
Asian School of Cyber Laws



A to Z of Cyber Crime

Asian School of Cyber Laws

Copyright notice

Legal notice

The information in this book is provided for informational purposes only and does not constitute legal advice.

This publication is part of the
Lexcode Education & Assessment Platform (LEAP) powered by:

LEXCODE

REGULATORY COMPLIANCE TECHNOLOGIES PVT. LTD.

Incubated by Science & Technology Park
promoted by Department of Science and Technology
Government of India

Contact us at:
Science and Technology Park, University of Pune, Pune-07
info@lexcode.in | www.lexcode.in

Established in 1999, Asian School of Cyber Laws is a global pioneer in cyber law and cyber crime investigation.

We have assisted the Government of India in framing draft rules and regulations under the Information Technology Act and drafting model rules for the functioning of Cyber Cafes and drafting the Information Age Crimes Act.

We have assisted the Controller of Certifying Authorities in drafting regulations relating to the recognition of foreign certifying authorities.

ASCL Computer Crime & Abuse Report (India) is the only study of its kind quoted by the United Nations in its E-commerce & Development Report (2003).

We were part of the Organizing Committee for the World Congress on Informatics and Law at Spain (2002), Cuba (2003) and Peru (2004).

Contact us at:
6th Floor, Pride Kumar Senate, Behind Sigma House,
Senapati Bapat Road, Pune - 411016 (India)
info@asianlaws.org | www.asianlaws.org

The most dangerous criminal may be the man gifted with reason, but with no morals.

Martin Luther King, Jr.,
The Purpose of Education, Maroon Tiger, January-February 1947

Contents

ONE

1. Anonymizer

People often surf the web under the illusion that their actions are private and anonymous. Unfortunately for them such is not the case.

Each time you visit a site, you leave a visiting card that reveals where you are coming from; what kind of computer you use; and various other details. Each visit of yours is logged!

An anonymizer or an anonymous proxy is a tool that attempts to make activity on the internet untraceable. It empowers you to surf the web without revealing any personal information. Not only does it hide your IP address and internet history but also unblocks the restricted websites and lets you navigate past web-filters.

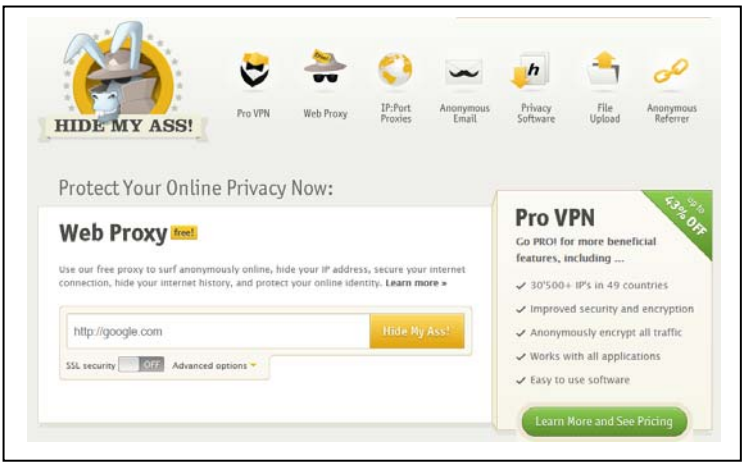
The problem arises when individuals use this to avoid the consequences of engaging in criminal, disruptive or socially unacceptable behavior online.

Illustration:

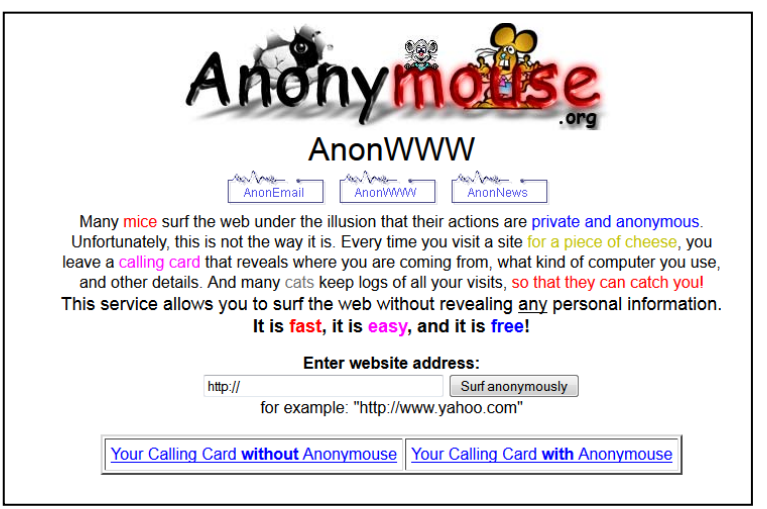
Sameer uses an anonymizer to log into an email spoofing website. He then sends out fraudulent emails to hundreds of people. When the police try to track the IP addresses in the email headers, they will trace it to the anonymizer and will not be able to track Sameer.

Illustration:

A school in Cochin had banned facebook usage from the computer lab. The school authorities had configured the firewall in a way that access to the site from school computers was blocked. Sameer, a student from the 8th grade, used an anonymizer to access facebook from the school computer.



Two popular anonymizers are hidemyass.com (above) and anonymouse.org (below).



TWO

2. ARP cache poisoning

Address Resolution Protocol (ARP) is how network devices associate MAC addresses with IP Addresses. This enables devices on a local computer network to find each other. ARP is similar to a roll call in school.

Every networked computer has 2 addresses - MAC address and IP address.

MAC address (Media Access Control) is a unique identifier e.g, 00-00-0c-34-11-4e that is usually hard-coded into a Network Interface Card (NIC) by its manufacturer. It does not change.

To know more about IP addresses, refer to the topic *IP Addresses, DNS* in the appendix.

ARP cache poisoning, also known as ARP spoofing is a technique in which an attacker sends fake ("spoofed") ARP messages onto a Local Area Network.

The aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway). This would send the traffic meant for gateway to the attacker.

ARP spoofing allows an attacker to intercept data (passwords, credit card numbers etc) being transmitted on the network.

Illustration :

Pooja uses her office computer to connect to an online shopping site. She enters her credit card number at the website thinking that the credit card information will be transmitted from her computer to the website through the default gateway of the office network.

Unknown to her, Sameer is carrying out an ARP cache poisoning on the office network. This results in the credit card information coming to his computer instead of going directly to the gateway.

3. Backdoor

Backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes. However, back doors are often used by attackers who detect and/or install it themselves.

Whether installed as an administrative tool or a means of attack; a back door poses as a security risk aiding crackers looking for vulnerable systems. Once the backdoor has been established by cyber criminals, they gain system entry giving them complete access to all kind of sensitive information of the victim such as his financial details, account numbers, passwords etc.

Such access enables the criminal to maliciously vandalize, alter, move, or delete files from the infected computer.

4. Backscatter

Also known as out scatter, backscatter is the side effect of email spam, worms and viruses.

This is best understood using a simple example. A worm sends out millions of spam emails using Sameer's email address as the sender. Thousands of these spam messages are addressed to non-existent email addresses. E.g. one such spam email is directed to pooja@example.com, a non-existent email address.

The example.com email server will reply to Sameer saying that the pooja@example.com email address is invalid.

This will result in Sameer getting thousands of emails.

5. The Blues- Bluebugging, Bluejacking and Bluesnarfing

Bluebugging, Bluejacking and Bluesnarfing are forms of attacks via Bluetooth. Initially a threat against laptops with bluetooth capability, these attacks later targeted mobile phones, PDAs and just about every device with Bluetooth capability.

Bluebugging allows a virtual takeover of the target phone. It manipulates the phone into compromising its security, so as to create a backdoor attack without notifying or alerting the phone's user, allowing the user to “take control” of a victim’s phone. Not only can the bluebugger make calls, send messages, read phonebooks, examine calendars but also eavesdrop on phone conversations.

The Bluebug program also has the capability to create a call forwarding application whereby the hacker receives calls intended for the target phone. A bluebug user can simply listen to any conversation his victim is having in real life.

Earlier the range for such an attack was 10 to 20 metres, however now the operational range has been increased with the advent of directional antennas.

A milder version of Bluebugging is **Bluejacking**. It involves sending anonymous, unwanted messages to other users with Bluetooth-enabled mobile phones or laptops.

Bluejacking depends on the ability of Bluetooth phones to detect and contact other Bluetooth devices nearby. The Bluejacker uses a feature originally intended for exchanging contact details or electronic business cards. He or she adds a new entry in the phone's address book, types in a message, and chooses to send it via Bluetooth. The phone searches for other Bluetooth phones and, if it finds one, sends the message.

Despite its name, Bluejacking is essentially harmless since the Bluejacker does not steal personal information or take control of your phone.

But Bluejacking can be a problem if it is used to send obscene or threatening messages or by criminals who could resort to this form of communication.

Bluesnarfing is the theft of data from a Bluetooth phone. The attacker, just by running the right software on their laptop, can discover a nearby phone, connect to it without confirmation and download essentials such as phonebook, emails, pictures and private videos, calendar and even the mobile phone's serial number to clone the entire phone.

Even by turning off the bluetooth, the potential victim cannot be safe from the possibility of being Bluesnarfed. As a device in

"hidden" status may also be Bluesnarfable by guessing the device's MAC address via a brute force attack. As with all brute force attacks, the main obstacle to this approach is the sheer number of possible MAC addresses.

BT Crawler is a scanner for Windows Mobile Based devices that implements Bluejacking and BlueSnarfing attacks.

6. Buffer overflow

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it is intended to hold. Since buffers are created to contain a limited amount of data; the extra information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

Buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions. This could in effect send new instructions to the attacked computer which in-turn could damage the user's files, change data, or disclose confidential information.

Buffer overflow attacks are said to have arisen because "the C programming language supplied the framework, and poor programming practices supplied the vulnerability".

Illustration:

Several years ago, a vulnerability to buffer overflow attack was discovered in Microsoft Outlook and Outlook Express. A programming flaw made it possible for an attacker to compromise the integrity of the target computer by simply sending an e-mail message.

Unlike the typical e-mail virus, users could not protect themselves by not opening attached files; in fact, the user did not even have to open the message to enable the attack.

The programs' message header mechanisms had a defect that made it possible for senders to overflow the area with extraneous data.

This allowed the attacker to execute whatever type of code they desired on the recipient's computers. Since the process was activated as soon as the recipient downloaded the message from the server, this type of buffer overflow attack was very difficult to defend. Microsoft has since created a patch to eliminate the vulnerability.

(Source: http://searchsecurity.techtarget.com)

7. Bullying in Cyberspace

Cyberbullying is when the Internet and related technologies are used to bully other people, in a deliberate, repeated, and hostile manner. This could be done via

1. text messages or images,

2. personal remarks posted online,

3. hate speeches,

4. instigating others to dislike and gang up on the target by making them the subject of ridicule in forums, and

5. posting false statements in order to humiliate or embarrass another person.

Cyberbullies may also disclose victims' personal data (e.g. real name, address, or workplace/schools) on websites.

Cases of piggy-backing on victim's identity are now common. This could be used to publish objectionable material in their name that defames or ridicules a subject.

A Legislation geared at penalizing cyberbullying has been introduced in a number of U.S. states including New York, Missouri, Rhode Island and Maryland. At least US seven states passed laws against digital harassment in 2007. In August 2008, the California state legislature passed one of the first laws in the USA to deal directly with cyberbullying.

Under the Indian law, cyber-bullying is covered by section 66A of the Information Technology Act. This section is titled "Punishment for sending offensive messages through communication service, etc."

This section provides for imprisonment upto 3 years and fine. Section 66A penalises the following being sent through email, sms etc:

(1) information that is grossly offensive or has menacing character; or

(2) false information sent for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will.

This section also penalises the sending of emails (this would include attachments in text, image, audio, video as well as any additional electronic record transmitted with the message.) for the following purposes:

(1) causing annoyance, or

(2) causing inconvenience, or

(3) to deceive or to mislead about the origin of the messages.

Illustrations:

Megan Taylor Meier was an American teenager from who committed suicide by hanging herself 3 weeks before her 14th birthday. A year later, Meier's parents prompted an investigation into the matter and her suicide was attributed to cyber-bullying through the social networking website MySpace.

An 8 year old girl from UK got into a fight with another girl. This resulted in the 8 year old being cyber bullied for more than 5 years! When the victim turned 14, she finally told her parents who got the messages stopped. Soon after that the victim was mugged and attacked by the bully and her friends. The victim was hospitalized for a week.

8. Click fraud

Click-fraud is occurs when a person (or an automated computer program) sham-clicks on a pay-per-click advertisement. This is done for the purpose of generating a charge per click without having an actual interest in the ad's content.

Click fraud is done by companies to deplete their competitor's advertising budget or by websites to gain revenue.

Some web sites pay people from remote places to make fraudulent clicks on an ad in order to inflate their customer's bills.

Click bots can also be used for click fraud. These small pieces of code can be spread like viruses on many computers in order to generate clicks from different IP addresses. The most intelligent scams involve a malware that adopts a low profile and generates only a few clicks per computer in order to avoid detection. These bots are generally controlled remotely by the person who wishes to limit the clicks to ads that can generate a real profit.

Click fraud, is hard to detect in the beginning but can be spotted eventually. The reason is that sham-clicks increase an advertiser's pay-per-click fees but don't generate sales.

Illustration

Several marketers sued Facebook for click fraud last year.

Facebook is arguing that the litigation should be dismissed because its contract with marketers provides that they must pay for all clicks, regardless of their validity.

Contrary to plaintiffs' allegations, the contract does not require Facebook to police its website for all instances of click fraud nor does it limit Facebook's ability to collect fees generated by clicks on plaintiffs' advertisements.

9. Computer trespass

A person is guilty of computer trespass if he or she intentionally and without authorization

1. accesses,
2. alters,
3. deletes,
4. damages,
5. destroys, or
6. disrupts

any computer, computer system, computer network, computer program, or data.

There are state specific laws on the subject which vary from one state to another. However the key element for all computer trespass offenses is lack of authorization to access a computer or computer system.

Illustration:

Teja uses his former wife Shrini's password to access her confidential financial files; he is said to have

committed computer trespass. It does not matter if he has guessed the password or the files were not password protected.

Vijay suspects his wife Basanti to be cheating on him; he checks her e-mails without her consent and prints out incriminating e-mails to use in his divorce case against her. Not only are the e-mails not admissible in court, but he would be committing a serious offence of computer trespass.

10. Cookie Manipulation

A cookie is a small file or text-only string registered in the memory of a web browser. It is used to identify a website user. The term originates from a well-known computer science term that is used when describing an opaque piece of data held by an intermediary.

Illustration:

Sanya enters her username and password and logs into example.com. Example.com places a cookie in her browser.

Every time that Sanya connects to the example server (to send an email, read an email etc), example verifies her logged in status and identity based on the cookie in her browser.

Once Sanya logs out, the cookie is destroyed.

Websites use cookies to authenticate users (e.g. gmail.com) personalize data (e.g. My Yahoo or Excite), to assist customers with online sales or services (e.g. eBay.com or Amazon.com) or

merely for collecting statistical and demographic data (e.g. DoubleClick.com).

Cookies which are saved in the form of simple text files can be deleted. If you delete a cookie while your browser is open, it will be recreated when you close the browser. This is because all cookies are held in the memory of your browser till you close the browser.

You can set the options offered by your Internet browser to accept either all, some or none of the incoming cookies.

Your browser can be set to warn you before accepting cookies.

A sample cookie:

WT_FPCid=2606225312.30232428:lv=1340297056862:ss=1340297027078microsoft.com/108834925404163096677920584 1030930232533*MUID3EB7CCF35DD667392CFCCF7559D667 48microsoft.com/102425489404163037927919363512793023 2533*MC1GUID=34bf6934c01bf84b9ed7be056293a40e&HASH=3469&LV=20126&V=3&LU=1340255633975microsoft.com/1024157940083230966683194159929030232533*AI&I=AxUFAAAAAAD1BgAAEBuCIaRDSYlMEQ+AVjfwww!!microsoft.com/1024413656640032436600194175529030232533*

Many sites use cookies to implement access control schemes of various sorts. For example, a subscription site that requires a user name and password might pass a cookie back to your browser the first time you log in.

Thereafter, the site will give you access to restricted pages if your browser can produce a valid cookie, basically using the cookie as an admission ticket. This can have several advantages for the site, not the least of which is that it can avoid the overhead of looking up your user name and password in a database each and every time you access a page.

However, unless this type of system is implemented carefully, it may be vulnerable to exploitation. For instance, a hacker could use a packet sniffer (discussed later in this book) to intercept the cookie as it passes from your browser to the server and then use it to obtain free access to the site.

There are 6 parameters in a cookie.

- The name of the cookie,
- The value of the cookie,
- The expiration date of the cookie,
- The path the cookie is valid for,
- The domain the cookie is valid for,
- The requirement for a secure connection to use the cookie

Out of these, two are compulsory (i.e. its name and its value). A semicolon [;] separates each parameter when it is set explicitly.

1. Name, Value

The name and the value of the cookie can be set by pairing them together. e.g., Name=Sanya

2. Expires

This parameter allows you to set the lifetime of the cookie. e.g.,

expires=Sat, 25-Apr-2013 18:30:00 GMT

If the 'Expires' parameter is not set clearly or is not set at all then by default the expiry gets set to the end of the session. Although the length of the session can depend on the browsers and the servers, usually the length of a session is considered to be the time that the browser window remains open. This is the case even if the user is no longer at that website.

3. Path

Out of the four optional settings or parameters of a cookie, this is probably the most useful. This parameter establishes the URL path within which the cookie remains valid. If the user reaches pages which are not contained in this path then the browser can no longer use this cookie. e.g., path=/documents

Suppose the path of the cookie is not set explicitly, then by default it takes the path as the URL of the document that has created the cookie.

4. Domain

This extends the path parameter a little. What happens if a site uses multiple servers for one domain? It is here that it becomes important to specify the Domain parameter in such a way so as

to make the cookie accessible to any of the pages of these multiple servers. e.g., domain=www.asianlaws.net

It is possible to assign cookies to either an individual machine or to an entire Internet domain.

Remember that to be able to set a cookie for a domain, the server should be a member of that domain.

If the Domain parameter is not set explicitly, then by default the full domain of the document that has created the cookie is taken.

5. Secure

This parameter indicates that a cookie with this parameter should only be used under secure server condition, e.g. SSL (Secure Socket Layer).

11. Copyright infringement

According to the US Federal Bureau of Investigation:

> *It's an age-old crime: stealing.*
>
> *But it's not about picking a pocket or holding up a bank. It's robbing people of their ideas, inventions, and creative expressions—what's called intellectual property—everything from trade secrets and proprietary products and parts to movies and music and software.*
>
> *It's a growing threat—especially with the rise of digital technologies and Internet file sharing networks.*

Internet copyright infringement is a form of intellectual property theft, which can lead to significant security issues and legal penalties. If a person attempts to use or distribute another person's work, who has "exclusive rights" over it, without authorization, he may be found guilty of copyright infringement. The common internet copyright violations

involve illegal download of movies, music files and pirating software applications.

Posting a copyrighted work such as writing or graphics online without the permission of the owner may also constitute internet copyright infringement.

Illustration:

Sameer an amazing cook, makes a website (smartcooking.com) sharing his recipes. Siddharth makes another website (cookingsmart.com) and uses Sameer's recipes and content for the web site. This is copyright infringement.

12. Crap-flooding

Crap-flooding is a form of trolling online media (discussion websites, Usenet newsgroups etc) with nonsensical, insane, and / or repetitive postings in order to make it difficult for other users to read other postings and thus pushing back relevant information.

It can also be motivated by a desire to waste the targeted site's bandwidth and storage space with useless text.

Crapflooding can also be carried out via automated software, which could handle the task much quicker than doing so manually.

It is possible to flood a client off the network simply by sending them data faster than they can receive thereby causing a quit with the "max text exceeded" message.

13. Cyber Stalking

Cyber stalking refers to the use of the Internet, e-mail, or other electronic communications devices to stalk another person.

Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim's immediate family.

Cyber stalking is also referred to as online harassment and online abuse. A cyber-stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected.

The first U.S. cyber-stalking law went into effect in 1999 in California. Other states include prohibition against cyber-

stalking in their harassment or stalking legislation. In Florida, HB 479 was introduced in 2003 to ban cyber-stalking.

In the United Kingdom, the Malicious Communications Act (1998) classified cyber-stalking as a criminal offense.

Under the Indian law, cyber-stalking is covered by section 66A of the Information Technology Act. This section is titled "Punishment for sending offensive messages through communication service, etc."

This section provides for imprisonment upto 3 years and fine. Section 66A penalises the following being sent through email, sms etc:

(1) information that is grossly offensive or has menacing character; or

(2) false information sent for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will.

This section also penalises the sending of emails (this would include attachments in text, image, audio, video as well as any additional electronic record transmitted with the message.) for the following purposes:

(1) causing annoyance, or

(2) causing inconvenience, or

(3) to deceive or to mislead about the origin of the messages.

Illustration:

In 2003 a US woman sought protection after claiming that someone had provided her personal information (including her description and location) to men via an online dating service.

The victim discovered the identity theft when she was contacted by a man who said they had arranged a casual encounter through the Lavalife.com dating service.

Shortly thereafter she was contacted by a second man following chat with 'her' about arranging a separate encounter.

Illustration:

Mrs. Ritu Kohli complained to the police against the a person who was using her identity to chat over the Internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days.

Mrs. Kohli further complained that the person was chatting on the Net, using her name and giving her address and was talking obscene language.

The same person was also deliberately giving her telephone number to other chatters encouraging them to call Ritu Kohli at odd hours.

Consequently, Mrs Kohli received almost 40 calls in three days mostly at odd hours from as far away as Kuwait, Cochin, Bombay and Ahmedabad.

The said calls created havoc in the personal life and mental peace of Ritu Kohli who decided to report the matter.

Consequently, the IP addresses were traced and the police investigated the entire matter and ultimately arrested Manish Kathuria on the said complaint. Manish apparently pleaded guilty and was arrested.

Illustration:

In the first successful prosecution under the California (USA) cyber stalking law, prosecutors obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances.

He terrorized the 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized about being raped.

On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her.

Illustration:

An honours graduate from the University of San Diego in USA terrorized five female university students over the Internet for more than a year.

The victims received hundreds of violent and threatening e-mails, sometimes receiving four or five messages a day. The student, who pleaded guilty, told the police that he had committed the crimes because he thought the women were laughing at him and causing others to ridicule him.

In reality, the victims had never met him.

Illustration:

In 2005, a minor from Massachusetts (USA) was convicted in connection with approximately $1 million in victim damages.

Over a 15-month period, he had hacked into Internet and telephone service providers, stolen an individual's personal information and posted it on the Internet, and made bomb threats to many high schools.

14. Cyber Terrorism

Computer crime has hit mankind with unbelievable severity. Computer viruses, worms, Trojans, denial of service attacks, spoofing attacks and e-frauds have taken the real and virtual worlds by storm.

However, all these pale in the face of the most dreaded threat – that of cyber terrorism.

> *Cyber terrorism is the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.*

The above definition was proposed by Rohas Nagpal, President, Asian School of Cyber Laws in the paper titled *Cyber Terrorism in the context of Globalization* presented at World Congress For Informatics And Law II held in Madrid, Spain in 2002.

Illustration:

On November 26 2010, a group calling itself the Indian Cyber Army hacked the websites belonging to the Pakistan Army, Ministry of Foreign Affairs, Ministry of Education, Ministry of Finance, Pakistan Computer Bureau, Council of Islamic Ideology, etc. The attack was done as a revenge for the Mumbai terrorist attacks.

Illustration:

In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a US based Internet Service Provider (ISP) and damaged part of its record keeping system.

The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "you have yet to see true electronic terrorism. This is a promise."

Illustration:

In 1998, Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages.

E-mail was tied up and undeliverable to the ISP's users, and support lines were tied up with people who couldn't get their mail.

The protestors also spammed IGC staff and member accounts, clogged their Web page with bogus credit

card orders, and threatened to employ the same tactics against organizations using IGC services.

They demanded that IGC stop hosting the website for the Euskal Herria Journal, a New York-based publication supporting Basque independence.

Protestors said IGC supported terrorism because a section on the Web pages contained materials on the terrorist group ETA, which claimed responsibility for assassinations of Spanish political and security officials, and attacks on military installations.

IGC finally relented and pulled the site because of the "mail bombings."

Illustration:

In 1998, a 12-year-old boy successfully hacked into the controls for the huge Roosevelt Dam on the Salt River in Arizona, USA.

He might have released floodwaters that would have inundated Mesa and Tempe, endangering at least 1 million people.

Illustration:

In 2005, US security consultants reported that hackers were targeting the U.S. electric power grid and had gained access to U.S. utilities' electronic control systems.

Illustration:

In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.

Illustration:

During the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with denial-of-service attacks by hacktivists protesting the NATO bombings.

In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were also common.

Illustration:

Since December 1997, the Electronic Disturbance Theater (EDT) has been conducting Web sit-ins against various sites in support of the Mexican Zapatistas.

At a designated time, thousands of protestors point their browsers to a target site using software that floods the target with rapid and repeated download requests.

EDT's software has also been used by animal rights groups against organizations said to abuse animals. Electrohippies, another group of hacktivists, conducted Web sit-ins against the WTO when they met in Seattle in late 1999.

Illustration:

In 1994, a 16-year-old English boy took down some 100 U.S. defense systems.

Illustration:

In 1997, 35 computer specialists used hacking tools freely available on 1,900 web sites to shut down large segments of the US power grid. They also silenced the command and control system of the Pacific Command in Honolulu.

Illustration:

In 2000, Asian School of Cyber Laws was regularly attacked by Distributed Denial of Service attacks by "hactivists" propagating the "right to pornography". Asian School of Cyber Laws has spearheaded an international campaign against pornography on the Internet.

Illustration:

In 2001, in the backdrop of the downturn in US-China relationships, the Chinese hackers released the Code Red virus into the wild. This virus infected millions of

computers around the world and then used these computers to launch denial of service attacks on US web sites, prominently the web site of the White House.

Illustration:

In 2001, hackers broke into the U.S. Justice Department's web site and replaced the department's seal with a swastika, dubbed the agency the "United States Department of Injustice" and filled the page with obscene pictures.

15. Cyber Warfare

According to the McAfee Virtual Criminology Report 2007, 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities. Cyber warfare is the use of computers and the Internet in conducting warfare in cyberspace.

The McAfee Virtual Criminology Report states that "Evidence suggests that governments and government-allied groups are now using the Internet for espionage and cyber-attacks on the critical national infrastructure (financial markets, utility providers, air traffic control) of other countries".

Illustration:

In 2009, a cyber spy network called "GhostNet" accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world. GhostNet was reported to originate in China, although that country denied responsibility.

The following extract from Wikipedia explains the functioning of GhostNet as under:

Emails are sent to target organizations that contain contextually relevant information. These emails contain malicious attachments, that when opened, drop a Trojan horse on to the system.

This Trojan connects back to a control server, usually located in China, to receive commands. The infected computer will then execute the command specified by the control server.

Occasionally, the command specified by the control server will cause the infected computer to download and install a Trojan known as Gh0st Rat that allows attackers to gain complete, real-time control of computers running Microsoft Windows.

Such a computer can be controlled or inspected by attackers, and even has the ability to turn on camera and audio-recording functions of infected computers, enabling monitors to perform surveillance.

16. Data Diddling

One of the most common forms of computer crime is data diddling - illegal or unauthorized data alteration. These changes can occur before and during data input or before output. Data diddling cases have affected banks, payrolls, inventory records, credit records, school transcripts and virtually all other forms of data processing known.

Data diddling is the changing of data before or during entry into the computer system for fun and profit. e.g. modifying grades, changing credit ratings, altering security clearance information, fixing salaries, or circumventing book-keeping and audit regulations, banks records, payrolls, inventory data, credit records, school transcripts, telephone switch configurations, and virtually all other applications of data processing.

This is one of the simplest methods of committing a computer-related crime, because it requires almost no computer skills whatsoever. Despite the ease of committing the crime, the cost can be considerable.

Illustration:

The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the New Delhi Municipal Council.

Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional.

He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

Illustration:

A keyboard operator processing orders at an Oakland USA department store changed some delivery addresses and diverted several thousand dollars worth of store goods into the hands of accomplices.

Illustration:

A ticket clerk at the Arizona Veterans' Memorial Coliseum in USA issued full-price basketball tickets, sold them and then, tapping out codes on her computer keyboard, recorded the transactions as half-price sales.

Illustration:

Sahil had a presentation stored on his computer for his company's meeting. Rohan was jealous of Sahil and

intended to cause harm. Hence, Rohan altered Sahil's presentation with junk data, in-order to catch Sahil offguard and in a potentially embarrassing/job threatening situation.

Illustration:

Two employees of a utility company found that there was a time lapse of several days between when meter readings were entered into the computer and when the bills were printed.

By changing the reading during this period, they were able to substantially reduce their electric bills and the bills of some of their friends and neighbors.

Illustration:

In the move 3 Idiots, two characters replace the hindi word "*chamatkaar*" with the word "*baladkaar*" in a speech being composed on a computer.

17. Data Leakage

A data leak is the uncontrolled, unauthorized transmission of classified information or release of secure information to an un-trusted environment. Other terms for this phenomenon include unintentional information disclosure, data breach and also data spill. Incidents range from concerted attack with the backing of organized crime or national governments to careless disposal of used computer equipment or data storage media.

Data breaches may involve financial information such as credit card or bank details, personal health information, personally identifiable information, trade secrets of corporations or intellectual property

Two individual groups are pursuing claims against Apple who claim that applications better known as ‘apps’ for the iPad and iPhone leak personally identifiable data.

18. Defamation

A person's reputation is his or her property and sometimes even more valuable than physical property.

Defamation is injury to the reputation of a person. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet. e.g. Sameer publishes defamatory matter about Pooja on a website or sends e-mails containing defamatory information to Pooja's friends.

The three essentials of defamation are:

1. the statement must be false and defamatory,

2. the said statement must refer to the victim, and

3. the statement must be published.

Illustration:

Rahul puts up a blog where he writes a false article holding Suman responsible for the murder of Sonia.

This harms the reputation of Suman. Rahul has committed an offence of cyber defamation.

Illustration:

Tuile, an anonymous online group posts false information about Row & Row company on the message board of their website which leads directly to a decrease in stock price or the cancellation of a key deal. This is cyber defamation.

Illustration:

Abhishek, a teenaged student was arrested by the Thane police in India following a girl's complaint about tarnishing her image in the social networking site Orkut.

Abhishek had allegedly created a fake account in the name of the girl with her mobile number posted on the profile.

The profile had been sketched in such a way that it drew lewd comments from many who visited her profile. The Thane Cyber Cell tracked down Abhishek from the false e-mail id that he had created to open up the account.

Illustration:

The Aurangabad bench of the Bombay high court issued a notice to Google.com following a public interest litigation initiated by a young lawyer.

The lawyer took exception to a community called 'We hate India', owned by someone who identified himself as Miroslav Stankovic. The community featured a picture of the Indian flag being burnt.

Illustration:

Unidentified persons posted obscene photographs and contact details of a Delhi school girl. Suggestive names like 'sex teacher' were posted on the profile.

The matter came to light after the girl's family started receiving vulgar calls referring to Orkut. Two strangers even came knocking at their door, telling them that the girl had invited them for sex through the Internet.

19. DOS / DDOS

This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource.

One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable.

DoS attacks are generally implemented by:

1. forcing the targeted computer(s) to reset, or consume its resources such that it can no longer provide its intended service; and/or,

2. obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread.

It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support thereby making the servers crash.

Illustration:

A series of distributed denial of service attacks in February 2000 crippled many popular websites including yahoo.com, amazon.com and cnn.com

Illustration:

A series of more than 125 separate but coordinated denial of service attacks hit the cyber infrastructure of Estonia in early 2007. The attacks were apparently connected with protests against the Estonian government's decision to remove a Soviet-era war memorial from the capital city. It is suspected that the attacks were carried out by Russian hackers. The attack lasted several days.

20. DNS poisoning

Domain Name System (DNS) poisoning attack, also called DNS spoofing, is when an attacker is able to redirect a victim to different website than the address that he types into his browser.

To learn more about DNS view the appendix topic titled *IP addresses, DNS*.

For example, a user types www.google.com into his browser, but instead of being directed to Google's servers he is instead sent to a fraudulent site that may look like Google's site but is in actuality controlled by an attacker.

The attacker is able to do this by changing the Internet Protocol (IP) address that usually points to Google to the fake IP address of the attacker.

A DNS Poisoning attack is in essence, tricking the DNS Server into sending traffic in the wrong direction – by adding false content in the DNS cache.

With cache poisoning an attacker attempts to insert into the DNS a fake address record for an Internet domain. If the server accepts the fake record, the cache is poisoned.

Subsequent requests for the address of the domain are answered with the address of a server controlled by the attacker.

As long as the fake entry is cached by the server subscriber's browsers or e-mail servers will automatically go to the address provided by the compromised DNS server.

At that point, a worm, spyware, Web browser hijacking program, or other malware can be downloaded to the user's computer from the rogue location.

Illustration:

Roar an internet criminal gang, poisons the DNS by changing the IP address of Bank Of Anguria website.

The customers of the bank are re-routed to another site looking just like the Banks site. A Trojan is downloaded here at this fake site on the clients computer. By infecting the clients computer all his confidential data as at the mercy of the Roar.

21. Easter Eggs

The failure of software testing is open for all to see at the Easter Egg Archive (www.eeggs.com)

According to the Archive, an Easter egg is “a hidden feature or novelty that the programmers have put in their software. In general, it is any hidden, entertaining thing that a creator hides in their creation only for their own personal reasons. This can be anything from a hidden list of the developers, to hidden commands, to jokes, to funny animations”.

A true Easter egg must satisfy the following criteria:

1. It should be undocumented, hidden, and non-obvious

An Easter Egg can't be a legitimate feature of a product, or be an obvious part of a storyline. Easter Eggs will usually stand out either because they totally don't fit with their context (like a pinball game in a word processor), or because they have a deeper hidden personal meaning to the creators, so they threw it in for entertainment.

2. It must be reproducible

Every user with the same product or combination of products must be able to produce the same result given the instructions.

3. It must have been put there by the creators for personal reasons

The Egg must have been put there on purpose, and furthermore have a personal significance to the creators beyond just making a better product (movie, TV show, software program, etc).

By definition, Easter Eggs are intended to be entertaining and harmless. However, an Easter Egg might be accidentally harmful, e.g. maybe there was a bug in the programmer's Easter Egg code, and in certain situations it might crash the program, or even the whole computer, forcing a reboot.

Some Easter Eggs:

1. Simply press Alt + Shift + 2 to win the Solitaire game on a Windows computer.

2. Open a new word document using Microsoft Word. Type the following:

=rand(200,99)

and then press enter. In a few seconds, you will see hundreds of pages filled with the sentence “The quick brown fox jumps over the lazy dog” repeated over and over!

An Easter Egg is a form of Trojan horse. If software developers can sneak a benign Easter Egg past the software testing and quality assurance teams, there's no doubt that they could similarly get a Trojan horse or intentional buffer overflow past them as well.

In fact, the attacker could even put the backdoor inside an Easter egg embedded within the main program.

The existence of Easter eggs proves quite clearly that a malicious developer or tester could put a nasty hidden functionality inside the product code and get it through product release without being noticed.

22. Email Spoofing

A spoofed email is one that appears to originate from one source but actually has been sent from another source e.g Pooja has an e-mail address pooja@asianlaws.org.

Her ex-boyfriend, Sameer spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Pooja, her friends may take offence and relationships may be spoiled for life.

Illustration:

In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold.

This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly.

Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

Illustration:

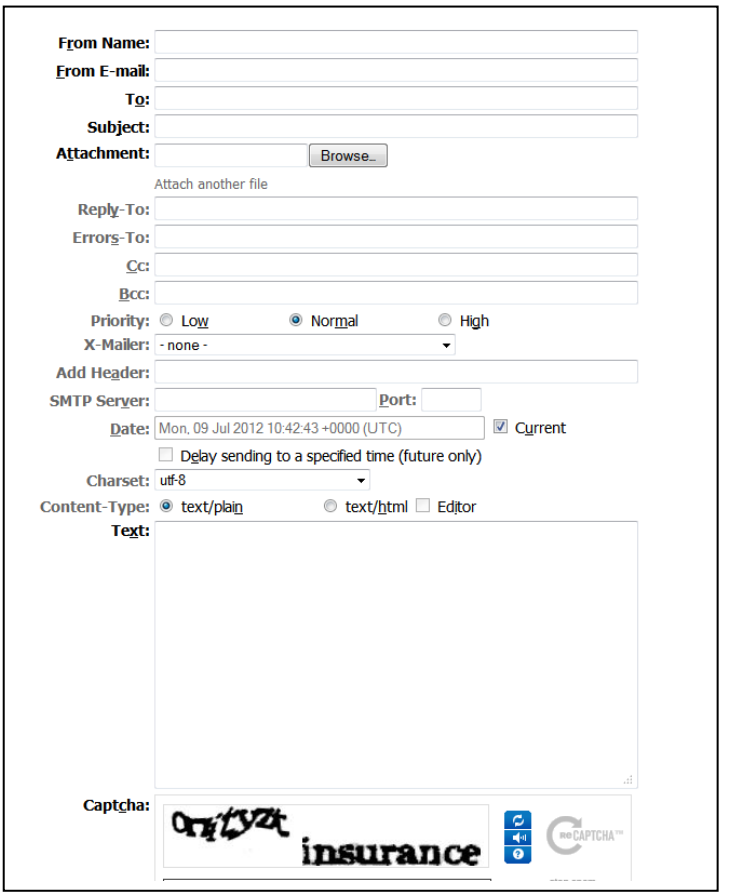
A branch of the erstwhile Global Trust Bank in India experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts.

An investigation revealed that someone had sent out spoofed emails to many of the bank's customers stating that the bank was in very bad shape financially and could close operations at any time. The spoofed email appeared to have originated from the bank itself.

Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitation and is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

One popular email spoofing site is: http://emkei.cz (screenshot shown below)


FAKE MAILER


From Name:
From E-mail:
To:
Subject:
Attachment:
Browse...
Attach another file
Reply-To:
Errors-To:
Cc:
Bcc:
Priority: Low Normal High
X-Mailer: - none -
Add Header:
SMTP Server:
Port:
Date: Mon, 09 Jul 2012 10:42:43 +0000 (UTC)
Current
Delay sending to a specified time (future only)
Charset: utf-8
Content-Type: text/plain text/html Editor
Text:
Captcha:
insurance

23. Encryption use by terrorists

A disturbing trend that is emerging nowadays is the increasing use of encryption, high-frequency encrypted voice/data links, encryption software like Pretty Good Privacy (PGP) etc by terrorists and members of organized crime cartels.

Strong encryption is the criminal's best friend and the policeman's worst enemy.

If a criminal were to use 512-bit symmetric encryption, how long would it take to decrypt the information using brute force techniques?

Suppose that every atom in the known universe (there are estimated to be 2300 of them) becomes a computer capable of checking 2300 keys per second, then it would take 2162 millennia to search 1% of the key space of a 512-bit key. The universe is believed to have come into existence less than 224 years ago.

Illustration:

Leary, who was sentenced to 94 years in prison for setting off fire bombs in the New York (USA) subway system in 1995, had developed his own algorithm for encrypting the files on his computer.

Illustration:

The Cali cartel is reputed to be using

• sophisticated encryption to conceal their telephone communications,

• radios that distort voices,

• video phones which provide visual authentication of the caller's identity, and

• instruments for scrambling transmissions from computer modems.

Illustration:

The Italian mafia is believed to use PGP.

Illustration:

On March 20, 1995, the Aum Supreme Truth cult dropped bags of sarin nerve gas in the Tokyo subway, killing 12 people and injuring 6,000 more.

Members of the cult had developed many chemical and biological weapons, including Sarin, VX, Mustard gas, Cyanide, botulism, anthrax and Q fever.

It is believed that preparations were underway to develop nuclear capability. The cult was also believed to be developing a "death ray" that could destroy all life!

The records of the cult had been stored in encrypted form (using the RSA algorithm) on computers.

The enforcement authorities were able to decrypt the information as the relevant private key was found in a floppy disk seized from the cult's premises. The encrypted information related to plans of the cult to cause mass deaths in Japan and USA.

Illustration:

In 1997, a Bolivian terrorist organization had assassinated four U.S. army personnel. A raid on one of the hideouts of the terrorists yielded information encrypted using symmetric encryption. A 12-hour brute force attack resulted in the decryption of the information and subsequently led to one of the largest drug busts in Bolivian history and the arrest of the terrorists.

Illustration:

James Bell was arrested for violating internal revenue laws of the USA. He did this by:

1. collecting the names and home addresses of agents and employees of the Internal Revenue Service (IRS) of the USA in order to intimidate them

2. soliciting people to join in a scheme known as "Assassination Politics". Under this scheme those who killed selected government employees, including tax collectors, would be rewarded;

3. using false Social Security Numbers to hide his assets and avoid taxes;

4. contaminating an area outside IRS premises in many states of the USA with Mercaptan (a stink gas).

Investigators found on his computer documents relating to a plan to destroy electronic equipment with nickel-plated carbon fiber.

They also found an invoice for the purchase of the fiber at his residence, and a bundle of the material at the residence of his associate, Robert East. Bell had exchanged PGP-encrypted e-mail messages with some of his associates.

As part of his plea bargain, he turned over the passphrase to his private key. This allowed investigators to decrypt messages that he had received.

Illustration:

Dutch organized crime syndicates use PGP and PGPfone to encrypt their communications. They also use

palmtop computers installed with Secure Device, a Dutch software product for encrypting data with International Data Encryption Algorithm (IDEA).

In 1995, the Amsterdam Police captured a PC in possession of one organized crime member. The PC contained an encrypted partition, which they were able to recover only in 1997.

Illustration:

An encryption case occurring in Vilseck, West Germany involved theft, fraud, and embezzlement of U.S. defense contractor and U.S. government funds from 1986 to 1988.

The accused had stored financial records relating to the crimes on a personal computer, the hard disk of which had been password protected.

The police used hacking software to defeat the password protection, only to find that some of the files listed in the directory had been encrypted.

They then found the encryption program on the hard disk and used brute force tools to decrypt the files.

Illustration:

The Dallas Police Department in the USA encountered encryption in the investigation of a drug ring, which was operating in several states of the USA and dealing in Ecstasy.

A member of the ring, residing within their jurisdiction, had encrypted his address book. He turned over the password, enabling the police to decrypt the file.

Meanwhile, however, the accused was out on bail and alerted his associates, so the decrypted information was not as useful as it might have been.

The police noted that Ecstasy dealers were more knowledgeable about computers when compared with other types of drug dealers, most likely because they were younger and better educated.

Illustration:

Kevin Poulson was a skilled hacker who rigged radio contests and burglarized telephone-switching offices and hacked into the telephone network in order to determine whose phone was being tapped and to install his own phone tapping devices.

Poulson had encrypted files documenting everything from the phone tapping he had discovered to the dossiers he had compiled about his enemies. The files had been encrypted several times using the Data Encryption Standard.

A US Department of Energy supercomputer took several months to find the key, at a cost of millions of dollars. The result yielded nearly ten thousand pages of evidence.

Illustration:

The mother of a 15-year old boy filed a complaint against an adult who had sold her son US $ 1000 worth of hardware and software for one dollar.

The man had also given the boy lewd pictures on floppy disks.

The man subsequently mailed the boy pornographic material on floppy disks and sent pornographic files over the Internet.

When the accused was arrested it was found out that he had encrypted a directory on the system using PGP. The police were never able to decrypt the files.

24. eShoplifting

Shoplifting is the act of stealing goods that are on display in a store. Simply put, e-shoplifting is the act of stealing goods that are available through an electronic store.

An eShop combines business logic and technology. Hackers target the vulnerabilities in the technology to buy products and services at lower prices (or even for free).

Some of the major causes of weaknesses in eShops are:

1. Poor input validation – This implies that the input of the user is not being properly sanitized or checked. Instead of entering his username, a user could enter some malicious code that could exploit the system.

2. Inappropriate utilization of cookies – This implies that the cookies are vulnerable to exploitation. The hacker could manipulate important values stored in the cookies.

3. Improper session or state tracking – This implies that the methodology used to track logged in users and their activities is not adequate.

4. Weakness in client-side scripting – Client side scripting is the class of computer programs on the web that are executed "client-side" (by the user's web browser), instead of server-side (on the web server). A hacker can manipulate the client side scripting to pass on malicious code to the eShop.

5. Poor database integration – This implies that the database storing all the information is not securely integrated with the front end and other sections of the eShop. This can lead to information being stolen while it is being passed on to or from the database. It could also lead to the user passing malicious code into the database.

6. Security flaws in third-party products – Flaws in third party products such as payment gateways can lead to the eShop being compromised.

TWENTY FIVE

25. Financial Crimes

Money is the most common motive behind all crime. The same is also true for cyber crime. Globally it is being observed that more and more cyber crimes are being committed for financial motives rather than for "revenge" or for "fun".

With the tremendous increase in the use of internet and mobile banking, online share trading, dematerialization of shares and securities, this trend is likely to increase unabated. Financial crimes include cyber cheating, credit card frauds, money laundering, hacking into bank servers, computer manipulation, accounting scams etc.

Illustration:

Punjab National Bank in India was cheated to the tune of Rs. 13.9 million through false debits and credits in computerized accounts.

Illustration: Rs. 2,50,000 were misappropriated from Bank of Baroda in India through falsification of computerized bank accounts.

Illustration:

The Hyderabad police in India arrested an unemployed computer operator and his friend, a steward in a prominent five-star hotel, for stealing and misusing credit card numbers belonging to hotel customers.

The steward noted down the various details of the credit cards, which were handed by clients of the hotel for paying their bills. Then, he passed all the details to his computer operator friend who used the details to make online purchases on various websites.

Illustration:

In 2004, the US Secret Service investigated and shut down an online organization that trafficked in around 1.7 million stolen credit cards and stolen identity information and documents.

This high-profile case, known as "Operation Firewall," focused on a criminal organization of some 4,000 members whose Web site functioned as a hub for identity theft activity.

Illustration:

In 2003, a hacker was convicted in the USA for causing losses of almost $25 million. The defendant pleaded

guilty to numerous charges of conspiracy, computer intrusion, computer fraud, credit card fraud, wire fraud, and extortion.

The hacker and his accomplices from Russia had stolen usernames, passwords, credit card information, and other financial data by hacking into computers of US citizens. They would then extort money from those victims with the threat of deleting their data and destroying their computer systems.

TWENTY SIX

26. Fire Sale

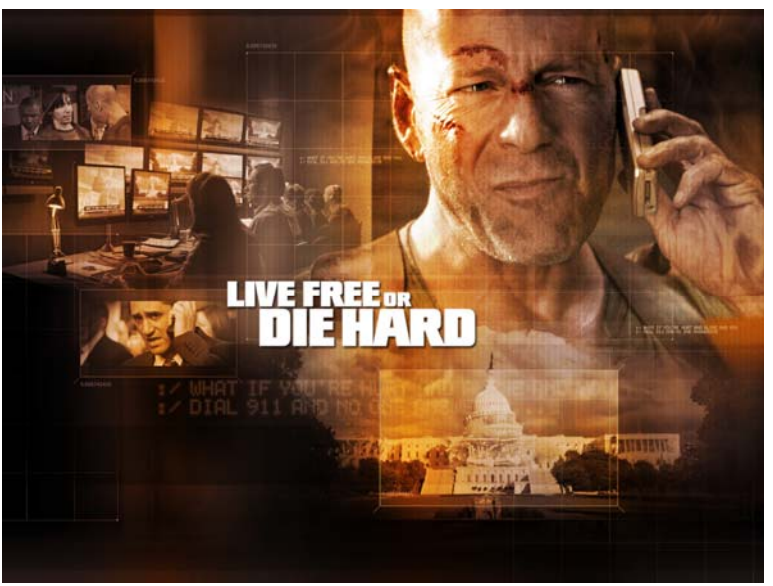
Fire sale is an attack designed to target the nation's reliance on computer controls. The attack procedure is known as a "fire sale" describing a three-stage coordinated attack on a country's transportation, telecommunications, financial, and utilities infrastructure systems. The attacks are designed to promote chaos and foster a leaderless environment. The term "fire sale" is used because "everything must go".

The first part of a fire sale consists of shutting down transportation, street signals, aircraft, highways, trains. The goal for this first part of the attack is to throw the public into chaos, making roads inaccessible, possibly for preventing emergency services to assist.

The second part of the attack would consist of shutting down the financial system of a country, such as the stock market, government agencies, and local law enforcement.

The last part of a fire sale involves the termination of all utilities and telecommunications in the country including phones, satellite communications, electricity, water, nuclear, solar, and anything else that requires a power source.

The final result of all three steps completed would leave the country or community in total chaos, making it extremely vulnerable.



The movie Die Hard 4.0 is based on the concept of a fire sale.

27. Fire Walking

A firewall is a security tool (software or hardware) that controls the data that comes in or goes out of a protected computer or network. A firewall also hides details of the protected network from the outside world.

Fire-walking enables a hacker to map the services allowed through a firewall.

28. Footprinting

Footprinting is usually done for the purpose of finding ways to intrude into the target environment. It can reveal system vulnerabilities and improve the ease with which these can be exploited. The purpose is to learn as much as possible.

Footprinting is the process of collecting data about a target organization's technology framework for the process of planning an attack (or for securing against an attack).

Footprinting usually does not involve any active attack against the target, it only involves gathering of relevant information that can later be used to plan an attack.

1.1 Physical location and contact information

Source of information:

1. Corporate website,
2. Business directories,
3. Online directories,
4. Annual reports,
5. Publications etc

Potential use / misuse:

It can be used to plan a social engineering attack.

Illustration: The network administrator in a global software company received a set of beautifully packed CDs by courier. The CDs contained critical and non critical "security updates" from the company that developed the operating system that ran his company's servers. He installed the "updates" which in reality was Trojanized software. A subsequent hacking attack resulted in a millions of dollars worth of source code being stolen.

1.2 General information on the IT infrastructure

Source of information:

1. Red Herring Prospectus published by a company at the time of its Initial Public Offering (IPO).

These can be downloaded from:
www.sebi.gov.in

Potential use / misuse:

Can be used to plan a social engineering attack.

Illustration: The red herring prospectus of Deccan Aviation Ltd details its IT Infrastructure. The document discloses that Air Deccan has "centralised IT resources within its operations, under the coverage of an IT team which as of March 31, 2006 included 35 staff". The document also discloses that its "CRS resides on servers

hosted at InterGlobe's data centre located in Gurgaon, India". An interesting extract from the prospectus is:

> "The servers are connected with redundant Internet connections leased from BSNL and Bharti, as well as by HCL wireless loop to help maximise network availability. Connectivity is maintained using an automated router that switches from a primary BSNL connection to a backup Bharti connection in case of failure. If both the leased connections fail the HCL wireless loop is used to keep the site live. … the Air Deccan servers are kept isolated from other networks and a Cisco Pix 515e Firewall and LINUX firewall has been installed to extend network security".

1.3 IP addresses of servers

Source of information:

1. IP address of the web servers can be obtained by a whois search using www.who.is

2. IP address of the name servers, mail servers etc can be obtained by performing a DNS Lookup using www.iptools.com

Potential use / misuse:

Can be used to carry out port scanning to find out open ports, vulnerabilities etc. It can also be used to attack

the computers using automated hacking and penetration testing software e.g. metasploit, backtrack etc.

1.4 IP addresses of individual computers

Source of information:

1. Analysis of the headers of emails sent by employees of the target organization.

2. Readnotify.com Tracking of the emails sent to employees of the target organization.

Potential use / misuse:

Can be used to carry out port scanning to find out open ports, vulnerabilities etc. Can also be used to attack the computers using automated hacking and penetration testing software e.g. metasploit, backtrack etc.

1.5 Recent mergers, acquisitions, takeovers

Source of information:

Information about the target organization's recent mergers, acquisitions, takeovers, can be obtained from the target's website and also from websites of regulatory bodies and stock exchanges e.g. www.sebi.gov.in,, www.bseindia.com, www.nseindia.com, etc.

Potential use / misuse:

This information is relevant as it takes months after a merger / acquisition for networks of the merging organizations to 'harmonize'. During this period these networks are vulnerable.

1.6 Websites

Source of information:

Comments put by the web developers in the HTML or JavaScript code of the target website can be obtained from the target websites. The robots.txt file can be obtained from the website.

Advanced options of search engines such as www.google.com can be used to download word documents, excel files etc from the target website. These files contain important information as well as deleted data that can be recovered. The website can be downloaded using tools such as 'websleuth'.

Potential use / misuse:

This information obtained would point to vulnerabilities or loopholes that can be exploited.

1.7 Wireless network

Source of information:

War-driving is done using a GPS enabled phone along with a software such as AiroMap which can reveal the

target that is open or a weakly protected wireless networks.

Potential use / misuse:

This information can pin point the vulnerabilities or loopholes which can be exploited.

1.8 Other information

Source of information:

News items about any security breaches at the target organization can be obtained from news websites and specialsed search engines such as www.data64.cc and www.bugs.ms

Statutory declarations made to the Registrar of Companies, Stock Exchange, SEBI etc may be available from the relevant websites or can be obtained from the authorities directly. Traceroute can be performed.

Potential use / misuse:

This information can point to vulnerabilities or loopholes that can be exploited.

Traceroute is used to gather information about network infrastructure and IP ranges around a given host. Traceroute information can be used to map out the nodes are available on a target's network architecture and later to exploit vulnerable or compromised nodes/computers.

29. Fraud

Dear Mr. Justin Williams, I'm Vikas Manjit Singh from Punjab (India). I belong to a city named Ludhiana.

Mr. Williams, I am having a brother in Canada who is also named Justin Williams. He was adopted from my parents by some Mr. William Ram of Welland. Me and my mum came over to Canada to leave Justin to his new family (William Ram's Family). It happened in June 1985.

So Mr. Justin Williams, if you are the same person I'm talking about. Then please give me some time so that I can let you know the realities.

Imagine the thoughts going through Mr. Justin William's head after reading this email. Is he really adopted? Where are his birth parents? Is this email from his birth brother?

In reality, this is a scam email originating from a college in Sangroor (India)! Canadian citizens are targeted with these emails. If the targets start believing the sender to be their

brother, they are asked to send money so that their "brother" can travel to Canada with the proof of the victim's adoption!

This is one of the hundreds of email scams being perpetrated on the Internet. These scams are commonly referred to as 'Nigerian 419' scams. These scam emails are believed to originate from Nigeria and section 419 of the Nigerian Penal Code relates to cheating (like the famous section 420 of the Indian Penal Code).

The 419 letter scams originated in the early 1980s as the oil-based economy of Nigeria went downhill. In the 1990s, letter scams gave way to email scams.

In 2007, Asian School of Cyber Laws conducted a 3 month intensive investigation of hundreds of scam emails. The results were very surprising to say the least. Less than 10% of these emails had actually originated from Nigeria!

A majority of these emails (more than 60%) have originated from Israel, followed by the Netherlands, UK and other European countries. The "birth brother" email was the only one originating from India.

Most of these scam emails promise the receiver millions (or sometimes billions) of dollars. Most commonly the email says that some rich African bureaucrat or businessman or politician has died and left behind a lot of money.

The scamster states that the Government is going to confiscate the money. The only way out is to transfer the money to the bank account of the email recipient. All that the email recipient

has to do is send his bank account details. For this a generous fee of a few million dollars will be paid!

If someone actually falls for this scam and provides the bank details, he is sent some official looking documents relating to the bank transfer of a huge sum of money. Once the victim is convinced of the "genuineness" of the transaction, something appears to go wrong.

The victim is informed that a small amount of money (ranging from US$ 100 to 2500) is needed for bank charges or other paper work. This money is the motive behind the elaborate scam. Once the victim pays this money, the scamster disappears from the scene.

The lottery scam emails inform the recipient that he has won a million dollar lottery run by Microsoft, Yahoo or some other well known global company. The winner is asked to provide his bank details and pay a small sum for bank charges and other processing fees.

Another scam email begins with "This is to inform you that we are in possession of a consignment, deposited by British National Lottery which is to be couriered to you". The email asks for 470 pounds to be sent to the courier company so that the cheque for the lottery prize can be sent.

Another scam email comes with the subject line "Blessed is the hand that giveth". The sender claims to be a widow on her deathbed. She wants to donate her wealth to someone who will pray for her.

Another scam email comes from an "employee of the Euro Lottery". The "employee" claims to be in a position to carry out a lottery fraud and is willing to share the money with the email recipient.

What is common in all these scams is that scanned versions of official documents are emailed to potential victims. Once the victim is convinced of the genuineness of the transaction, a small fee is requested for meeting bank charges / legal fees / courier charges etc. It is this small fee that is the motive behind the scam.

It is believed that thousands of people are defrauded of billions of dollars every year through these scams.

Illustration:

In 2005, an Indian businessman received an email from the Vice President of a major African bank offering him a lucrative contract in return for a kickback of Rs 1 million.

The businessman had many telephonic conversations with the sender of the email. He also verified the email address of the 'Vice President' from the website of the bank and subsequently transferred the money to the bank account mentioned in the email.

It later turned out that the email was a spoofed one and was actually sent by an Indian based in Nigeria.

Illustration:

A new type of scam e-mail threatens to kill recipients if they do not pay thousands of dollars to the sender, who purports to be a hired assassin.

Replying to the e-mails just sends a signal to senders that they've reached a live account. It also escalates the intimidation.

In one case, a recipient responded that he wanted to be left alone and threatened to call authorities. The scammer, who was demanding an advance payment of $20,000, e-mailed back and reiterated the threat, this time with some personal details about the recipient—his work address, marital status, and daughter's full name.

Then an ultimatum:

"TELL ME NOW ARE YOU READY TO DO WHAT I SAID OR DO YOU WANT ME TO PROCEED WITH MY JOB? ANSWER YES/NO AND DON'T ASK ANY QUESTIONS!!!"

There is also a twist in the scam. E-mails are surfacing that claim to be from the FBI in London and inform recipients that an arrest was made in the case. The e-mail says the recipient's information was found on the suspect and that they should reply to help further the investigation. This, too, is a scam!

30. Online Gambling

There are thousands of websites that offer online gambling. The special issue with online gambling is that it is legalised in several countries. So legally the owners of these websites are safe in their home countries.

The legal issues arise when a person residing in a foreign country like India (where such websites are illegal) gambles on such a website.

Illustration

The website ladbrokes.com permits users to gamble on a variety of sports such as cricket, football, tennis, golf, motor racing, ice hockey, basketball, baseball, darts, snooker, boxing, athletics, rugby, volleyball, motor cycling etc.

Additionally it also features an online casino. The website has no technical measures in place to prohibit residents of certain countries (where online gambling is illegal) from betting at their website.

31. Google based hacking

Google, arguably the world's most popular and powerful search engine, can be easily misused by hackers. Malicious users can use the Google search engine extensively to gather confidential or sensitive information, which is not visible through common searches. There are several special commands of Google that can be used for critical information digging.

intitle:

The "intitle:" syntax helps Google restrict the search results to pages containing that word in the title. For example,

intitle: login password

This will return links to those pages that have the word "login" in their title, and the word "password" anywhere in the page.

Similarly, if there is a query for more than one word in the page title then in that case "allintitle:" can be used instead of "intitle" to get the list of pages containing all the words in its title. For example using

intitle: login intitle: password

This is same as querying allintitle: login password

These search syntax can be used to look for vulnerable sites

allintitle: “index of /root”

This will list down the links to the web server which gives access to restricted directories like “root” through web. This directory sometimes contains sensitive information which can be easily retrieved through simple web requests.

allintitle: "index of /admin”

This syntax will list down the links to the websites which have index browsing enabled for restricted directories like “admin” through the web. Most of the web applications use names like “admin” to store admin credentials in it. This directory sometimes contains sensitive information which can be easily retrieved through simple web requests.

Other illustrations are:

- intitle:"Index of" .sh_history
- intitle:"Index of" .bash_history
- intitle:"index of" passwd
- intitle:"index of" people.lst
- intitle:"index of" pwd.db
- intitle:"index of" etc/shadow

- intitle:"index of" spwd
- intitle:"index of" master.passwd
- intitle:"index of" htpasswd
- intitle:"index of" members OR accounts
- intitle:"index of" user_carts OR user_cart
- allintitle: sensitive filetype:doc
- allintitle: restricted filetype :mail
- allintitle: restricted filetype:doc site:gov

site:

The "site:" syntax restricts Google to query for certain keywords in a particular site or domain. For example:

Courses site:asianlaws.org

This will look for the keyword "courses" in those pages present in all the links of the domain "asianlaws.org". There should not be any space between "site:" and the "domain name".

inurl:

The "inurl:" syntax restricts the search results to those URLs containing the search keyword. For example:

inurl: passwd

This syntax will return only links to those pages that have "passwd" in the URL.

Similarly, if one has to query for more than one word in an URL then in that case “allinurl:” can be used instead of “inurl” to get the list of URLs containing all those search keywords in it. e.g.

allinurl: etc/passwd

This will look for the URLs containing “etc” and “passwd”. The slash (“/”) between the words will be ignored by Google.

These search syntax can be used to look for vulnerable sites

allinurl:winnt/system32/

This syntax will list down all the links to the server which give access to restricted directories like “system32” through the web. If access to cmd.exe in the “system32” directory is obtained, and if it can be executed, then the server would be compromised.

allinurl: wwwboard/passwd.txt

This syntax will list down all the links to the server which are vulnerable to “WWWBoard Password vulnerability”. To know more about this vulnerability, visit:

http://www.securiteam.com/exploits/2BUQ4S0SAW.html

inurl:.bash_history

This syntax will list down all the links to the server which give access to “.bash_history” file through web. This is a command history file.

This file includes the list of commands executed by the administrator, and sometimes includes sensitive information such as passwords typed in by the administrator. If this file is compromised and it contains the encrypted unix (or *nix) password then it can easily be cracked using tools like “John The Ripper”.

inurl: config.txt

will list down all the links to the servers which give access to “config.txt” file through web. This file contains sensitive information, including the hash value of the administrative password and database authentication credentials.

Other illustrations are:

- inurl:admin filetype:txt
- inurl:admin filetype:db
- inurl:admin filetype:cfg
- inurl:mysql filetype:cfg
- inurl:passwd filetype:txt
- inurl:iisadmin
- inurl:orders.txt
- inurl:"wwwroot/*."
- inurl:adpassword.txt
- inurl:webeditor.php

- inurl:file_upload.php
- inurl:gov filetype:xls "restricted"
- index of ftp +.mdb allinurl:/cgi-bin/ +mailto
- inurl:auth_user_file.txt

link:

The “link:” syntax will list down web pages that have links to the specified webpage. E.g.

link:www.asianlaws.org

This syntax lists the web pages that have links pointing to the AsianLaws.org homepage. Note that there can be no space between the "link:" and the web page URL.

filetype:

This “filetype:” syntax restricts Google search for files on the internet with particular extensions (i.e. doc, pdf or ppt etc). For example:

filetype:doc site:gov confidential

This syntax will look for files with “.doc” extension in all government domains with “.gov” extension and containing the word “confidential” either in the pages or in the “.doc” file. i.e. the result will contain the links to all confidential word document files on the government sites.

related:

This syntax will list web pages that are "similar" to a specified web page. For e.g.

related:www.asianlaws.org

This syntax will list web pages that are similar to the AsianLaws.org site. Note there can be no space between the "related:" and the web page URL.

cache:

The query “cache:” will show the version of the web page that Google has in its cache. For e.g.

cache:www.asianlaws.org

This syntax will show Google's cache of the AsianLaws.org homepage. Note there can be no space between the "cache:" and the web page URL.

If you include other words in the query, Google will highlight those words within the cached document. For e.g.

cache:www.asianlaws.org courses

This syntax will show the cached content with the word "courses" highlighted.

intext:

The “intext:” syntax searches for words in a particular website. It ignores links or URLs and page titles. e.g.

intext:exploits

This syntax will return only links to those web pages that have the search keyword "exploits" in its webpage.

phonebook:

The syntax “phonebook” searches for U.S. street address and phone number information. e.g.

phonebook:Lisa+CA

This syntax will list down all names of person having “Lisa” in their names and located in “California (CA)”. This can be used for collecting personal information for social engineering.

32. Griefers

A griefer is a player who does things in a game to deliberately cause annoyance or "grief" to another player.

Many subscription-based games actively oppose griefers, since they drive away business. It is common for developers to release server-side upgrades and patches to annul griefing methods.

Many online games employ game masters that reprimand offenders. Others have opted for a crowd sourcing approach, where players can report griefing. Malicious players are then red-flagged, and are dealt with at a gamemaster's discretion.

As many as 25% of customer support calls to companies operating online games deal specifically with griefing.

The ways of causing grief are:

1. **Player vs player abuse:** Singling out the same person and killing them over and over when they are defenseless until they log off.

2. **Kill stealing:** Repeatedly trying to steal another person kills so that their time is wasted.

3. **Verbal abuse:** Spamming a person with vulgar, hateful, or offensive messages.

4. **Blocking:** Getting in another's way so they cannot move or get out of a particular area.

5. **Training:** Triggering many monsters, almost always impossible to fight and survive, with the intention to either run someone out of an area or kill them indirectly if the server is not 'player vs player' enabled.

Illustration:

Second Life bans harassment (defined as being rude or threatening, making unwelcome sexual advances, or performing activities likely to annoy or alarm somebody) and assault (shooting, pushing, or shoving in a safe area, or creating scripts/scripted objects that target another user and hinder their enjoyment of Second Life) in its community standards.

Sanctions include warnings, suspension from Second Life, or being banned altogether.

33. Hactivism

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message.

It could be defined as "the use of legal and/or illegal digital tools in pursuit of political ends". Therefore it is politically- or ideologically-motivated vandalism.

A hacktivist uses the same tools and techniques as a hacker, but does so in order to disrupt services and bring attention to a political or social cause. For example, one might leave a highly visible message on the home page of a Web site that gets a lot of traffic or one that embodies a point-of-view that is being opposed. Also a hacktivist could launch of a denial-of-service attack to disrupt traffic at particular site.

Hacktivism uses cyber attacks based on political motivations who use cyber sabotage to promote a specific cause. As opposed to the hacking industry intent on data theft, hacktivism is not motivated by money and high visibility is the key objective. Hacktivisms are motivated by revenge, politics, ideology, protest and a desire to humiliate victims. The

question that arises here is, what is the point of embarrassing someone if you they didn't know who executed the attack?

Illustrations:

Microsoft's UK Event's website was displaced with a Saudi Arabian flag.

Hacktivists protesting against the Iranian election - In this DDoS attack, hacktivists operating from outside of Iran, targeted Iranian government and other state-sponsored websites. As a result, the Iranian government blocked access to different social network sites to prevent netizens from providing coverage regarding the current state of affairs on the street.

Russian hacktivists targeting Social Networks hosting Georgian blogger – By employing DDoS attacks, Russian hacktivists were able to bring down social network services such as Facebook and Twitter. This was their retaliation campaign against a controversial Georgian blogger who had accounts on these networks

A recent demonstration of hacktivism followed the death of a Chinese airman when his jet fighter collided with a U.S. surveillance plane in April 2001. Chinese and American hacktivists from both countries hacked Web sites and used them as "blackboards" for their statements.

34. Hijacking

Just as conventional hijacking of an airplane is done by using force, similarly web jacking means forcefully taking over control of a website. The motive is usually the same as hijacking – ransom. The perpetrators have either a monetary or political purpose which they try to satiate by holding the owners of the website to ransom.

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). There on the owner of the website does not have control over what appears on that website.

How does web jacking take place?

The administrator of any website has a password and a username known only to him (or someone authorized by him) which is used to upload files from his computer on the web server (simply put, a server is a powerful computer) on which his website is hosted.

Ideally, this password remains secret with the administrator. If a hacker gets hold of this username and password, then he can pretend to be the administrator.

As computers don't recognize people – only usernames and passwords it grants control of the website to whoever enters the correct password and username.

There are many ways in which a hacker may get to know a password, the most common being password cracking wherein a "cracking software" is used to guess a password. Password cracking attacks are most commonly of two types.

The first one is known as the dictionary attack. In this type of attack the software will attempt all the words contained in a predefined dictionary of words.

For example, it may try Rahim, Rahul, Rakesh, Ram, Reema, Reena … in a predefined dictionary of Indian names. These types of dictionaries are readily available on the Internet.

The other form of password cracking is by using 'brute force'. In this kind of attack the software tries to guess the password by trying out all possible combinations of numbers, symbols, letters till the correct password is found. For example, it may try out password combinations like abc123, acbd5679, sdj#%^, weuf*(-)*.

Some software, available for password cracking using the brute force technique, can check a huge number of password combinations per second. When compared with a dictionary attack, a brute force attack takes more time, but it is definitely more successful.

Illustration

In an incident reported in the USA, the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website. They demanded a ransom of 1 million dollars from her.

The owner, a schoolteacher, did not take the threat seriously. She felt that it was just a scare tactic and ignored the e-mail. It was three days later that she came to know, following many telephone calls from all over the country, that the hackers had web jacked her website. Subsequently, they had altered a portion of the website which was entitled 'How to have fun with goldfish'.

In all the places where it had been mentioned, they had replaced the word 'goldfish' with the word 'piranhas'.

Piranhas are tiny but extremely dangerous flesh-eating fish. Many children had visited the popular website and had believed what the contents of the website suggested.

These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured!

35. Identity Fraud

Identity theft is a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity. This is done typically in order to access resources or obtain credit and other benefits in that person's name.

The victim of identity theft can suffer adverse consequences if held accountable for the perpetrator's actions. Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number without permission and commits fraud or other crimes.

It’s a type of fraud which involves stealing money or gaining other benefits by pretending to be someone else. Having your identity stolen can be both financially and emotionally devastating.

Illustrations:

Helen made use of public records of individual citizens which were published in official registers obtained information about Hercules. She then bought a mobile connection on his name. Hence misuseing his identity.

Illustrations:

Kai Kai stole credit cards by pick pocketing and bought herself expensive jewellery using somebody else's name.

Illustration:

Bora Bora Bank failed to shred confidential information before throwing it into dumpsters. Mocambo stole their valuable information and wrote letters to other companies as the Director of the bank.

36. Impersonation

Online impersonation is one of the most dangerous kinds of online reputation problems. It happens when someone else assumes your identity and communicates using your real name, photograph or avatar.

Impersonator could either hack into your real accounts; or just create fake profiles or comments purporting to be "you." The motivation behind the act may be revenge, sadism, extortion, or playing some kind of twisted prank. The damage to reputation caused by impersonating someone online can be substantial and hard to cope with.

Illustration:

Aryan, dressed like a policeman and went to an Mrs. Fernandes house. She used to stay alone and was old. Aryan told her he was there for her security and she should give him all her valuables so he would safely keep them for her. Aryan ran away with all her valuables. This is a case of police impersonation.

Impersonation is a violation of the Twitter Rules. Twitter accounts pretending to be another person or entity in order to confuse or deceive can be permanently suspended under the Twitter Impersonation Policy.

37. Joe - Job

A Joe job is an e-mail spoofing exploit in which someone sends out huge volumes of spam that appear to be from someone other than the actual source. A Joe job is sometimes conducted as an act of revenge on someone who reports a spammer to their Internet service provider (ISP) or publicly advocates anti-spam legislation.

The perpetrator is said to be Joeing the legitimate owner of the e-mail address they use. The spammer may not have to do anything more than change the "Reply To" address in their e-mail program.

Essentially, a Joe Job is a very crude form of identity theft. Your email address is used as the "sender's address" in most cases. Users Website URL is advertised, but an especially diligent and vicious attacker may even use the users name in the signature of the message. The email will not only be sent to millions of addresses once, but also in a repeated loop to each recipient before the attack ends.

Therefore it is a spam attack using spoofed sender data. Aimed at tarnishing the reputation of the apparent sender and/or induce the recipients to take action against him.

Joe-jobbers could also be businesses trying to defame a competitor or a spammer trying to harm the reputation of an anti-spam group or filtering service. Joe job attacks in other media are often motivated politically or through personal enmity.

38. Key stroke Logging

Keystroke logging (often called keylogging or "keyloggers") is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. There are numerous keylogging methods, ranging from hardware and software-based approaches to electromagnetic and acoustic analysis.

A keylogger , is a hardware device or small program that monitors each keystroke a user types on a specific computer's keyboard. As a hardware device, a keylogger is a small battery-sized plug that serves as a connector between the user's keyboard and computer. Because the device resembles an ordinary keyboard plug, it is relatively easy for someone who wants to monitor a user's behavior to physically hide such a device "in plain sight."

As the user types, the device collects each keystroke and saves it as text in its own miniature hard drive. At a later point in time, the person who installed the keylogger must return and

physically remove the device in order to access the information the device has gathered.

A keylogger program does not require physical access to the user's computer. It can be downloaded on purpose by someone who wants to monitor activity on a particular computer or it can be downloaded unwittingly as spyware

39. Logic Bomb

A logic bomb is a piece of code intentionally inserted into a software system which when triggered will set off a malicious task such as reformatting, and/or deleting, altering or corrupting data on a hard drive. It's secretly inserted into the code of a computer's existing software, where it lies dormant until that event occurs.

A program in which damage is delivered when a particular logical condition occurs; e.g., not having the author's name in the payroll file. Logic bombs are a kind of Trojan Horse and most viruses are logic bombs.

Illustrations:

In October 2009, Douglas Duchak was terminated from his job as data analyst at the TSA's Colorado Springs Operations Center (CSOC). Surveillance cameras captured images of Duchak entering the facility after hours loading a logic bomb onto a CSOC server that stored data from the U.S. Marshals. In January 2011, Duchak was sentenced to two years prison, $60,587 in fines, and three years probation.

In June 2006 Roger Duronio, a disgruntled system administrator for financial company UBS PaineWebber charged with using a logic bomb to damage the company's computer network. He was also charged with securities fraud for his failed plan to drive down the company's stock with activation of the logic bomb.

Duronio was later convicted and sentenced to 8 years and 1 month in prison, as well as a USD 3.1 million restitution to UBS.

40. Lottery Scam

A lottery scam is a type of advance-fee fraud which begins with an unexpected email notification that says "You have won!" a large sum of money in a lottery.

The recipient of the message — the target of the scam — is usually told to keep the notice secret, "due to a mix-up in some of the names and numbers," and to contact a "claims agent." After contacting the agent, the target of the scam will be asked to pay "processing fees" or "transfer charges" so that the winnings can be distributed, but will never receive any lottery payment. Victims who do actually pay the requested fees will probably find that they receive continuing payment demands to cover "unexpected expenses".

The requests for money will go on until the victim realizes what is happening or has no further money to send. In some cases, the scammers give victims the option of opening an account at a particular bank as an alternative to paying upfront fees.

However, this "bank" which is completely bogus, will insist on an initial deposit of $3000 as a requirement for opening the account. The fake bank will have a legitimate looking website to reinforce the scam.

Many email lottery scams use the names of legitimate lottery organizations or other legitimate corporations/companies, but this does not mean the legitimate organizations are in any way involved with the scams.

Illustration:

A 35-year-old Nigerian identified as Ozoya Isaian (35) involved in the online lottery scam was arrested in Delhi for allegedly cheating people of crores of rupees. He was nabbed following investigations into a complaint filed by a Pune resident earlier this month. In the complaint, the man alleged that he was cheated of Rs 22 lakh after he responded to an SMS that claimed he had won a lottery in the UK.

Yahoo filed a lawsuit in 2008, after a Nigerian and Thai group invented the fake lottery scam tricking people into believing they had won prizes in a lottery organized by Yahoo. Yahoo has been awarded $610 million in a court judgment against the scammers.

An 89-year-old woman in Hillsborough, California, who believed she had won $7.5 million in the Australian Government Lottery and wired $70,000 to claim it. The money was sent to a secret “Swiss” account, which turned out to be in a Vancouver bank

41. Mail Bombing

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

Email bombing is a type of denial-of-service attack. A denial-of-service attack is one in which a flood of information requests is sent to a server, bringing the system to its knees and making the server difficult to access.

Illustration:

A British teenager was cleared of launching a denial-of-service attack against his former employer, in a ruling under the UK Computer Misuse Act.

The teenager was accused of sending 5 million e-mail messages to his ex-employer that caused the company's e-mail server to crash. The judge held that the UK Computer Misuse Act does not specifically include a denial-of-service attack as a criminal offence.

Illustration:

In one case, a foreigner who had been residing in Simla, India for almost 30 years wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India.

He decided to take his revenge. Consequently, he sent thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.

42. Malware

Malware, short for malicious software, is software used or created by hackers to infiltrate or damage or disrupt computer operation, gather sensitive information, or gain access to private computer systems. While it is often software, it can also appear in the form of scripts or code. 'Malware' is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software.

Malware includes computer viruses, worms, trojan horses, spyware, adware, most rootkits, and other malicious programs. In law, malware is sometimes known as a computer contaminant, as in the legal codes of several U.S. states. Some malware is disguised as genuine software, and may come from an official company website.

Malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others. It can also hijack your browser, redirect your search attempts, serve up nasty pop-up ads, track what web sites you visit etc. Malware is sometimes used broadly against corporations to gather guarded information, but also to disrupt their operation in

general. Many malwares will reinstall themselves even after you think you have removed them, or hide themselves deep within Windows, making them very difficult to clean.

Left un-guarded, personal and networked computers can be at considerable risk against malware threats.

43. Nigerian 419 Fraud Scheme

A Nigerian 419 scam is a confidence trick in which the target is persuaded to advance relatively small sums of money in the hope of realizing a much larger gain.

The term, "419" comes from the section of the Nigerian Penal Code outlawing fraudulent criminal activities by its citizens. While the scam is not limited to Nigeria, Nigerians have become so associated with this fraud that it is widely known as Nigerian scam or 419 scam. In 2005 Lagos in Nigeria was widely considered the world's leading place for scam crimes.

Few methods used :

A new scam targets people who have posted their resumes on job sites. The scammer sends a letter with a falsified company logo. The job offer usually indicates exceptional salary and benefits and requests that the victim needs a "work permit" for working in the country and includes the address of a (fake) "government official" to contact. The "government official" then proceeds to fleece the victim by extracting fees from the

unsuspecting user for the work permit and other fees till the victim realizes the scam.

A modern activity is advertising automobiles on websites. They list a (non-existent) high value car with a low price as bait to attract buyers eager to buy quickly.

The scammer says "I am not in the country, but if you pay me first, a friend will drive the car around to you". The payment required may be the full price, or a deposit, but it would not be an insignificant fee.

The victim never sees the car, as it does not exist. The scammers use email only, as they know that the sound of their voice and their attitude will give them away as being high risk.

The con artist approaches the victim on an online dating service, an Instant messenger, or a social networking site. The scammer claims an interest in the victim, and posts pictures of an attractive person.

The scammer uses this communication to gain confidence, and then asks for money. The con artist may claim to be interested in meeting the victim, but needs cash to book a plane, hotel room, or other expenses.

In other cases, they claim they're trapped in a foreign country and need assistance to return, to escape imprisonment by corrupt local officials, to pay for medical expenses due to an illness contracted abroad, and so on.

Illustration:

On January 5, 2012, a 65-year-old Korean man and his daughter, who is in her 30s, were lured to South Africa with a 419 scam.

They apparently responded to an email from individuals who promised them tens of millions of dollars. They were taken to a house in Meadowlands in Soweto where they were held, with the driver, while the kidnappers demanded a ransom from their family in South Korea. The man's wife, in South Korea, contacted the South Korean embassy in South Africa. At the same time the driver escaped and alerted local police. Both were rescued by police.

Illustration:

In February 2003, Jiří Pasovský, a 72 year-old scam victim from the Czech Republic, shot and killed 50-year old Michael Lekara Wayid, an official at the Nigerian embassy in Prague, and injured another person, after the Nigerian Consul General explained he could not return $600,000 that Pasovský had lost to a Nigerian scammer.

44. Packet Sniffing

All network data travels across the Internet, and then into and out of PCs, in the form of individual, variable size, "data packets". Since the typical PC user never "sees" any of this raw data, many spyware systems covertly send sensitive information out of the user's computer without their knowledge.

Packet sniffing is a method of tapping each packet as it flows across the network i.e., it is a technique, in which a user sniffs data belonging to other users of the network. Packet sniffers can be used as an administrative tool or as a hacking tool. It depends on the user.

Network sniffers can capture passwords and other sensitive pieces of information passing through the network.

45. Phishing & Spoofing attacks

Jasa dista tasa nasta mahnun jag phasta (old Marathi saying)
[Things are not what they seem and that is why
the world gets conned]

In the 19th century, British comedian Arthur Roberts invented a game called Spoof, which involved trickery and nonsense. This gave the English speaking world a new word that today symbolizes a gamut of hacking technologies.

Spoofing attacks primarily include e-mail spoofing, SMS spoofing, IP spoofing, and web spoofing. Spoofing attacks are used to trick people into divulging confidential information (e.g. credit card data) or doing something that they would usually not do (e.g. installing malicious software on their own computers).

Such use of spoofing attacks is commonly referred to as Phishing.

Sending an e-mail from somebody else's e-mail ID is the simplest form of **Email spoofing**. Innumerable tools exist on the Internet which can easily be used to send e-mails appearing to have been sent by somebody else. The effects are intense.

> **Case:** Many customers received an email from their bank asking them to verify their usernames and passwords for the bank records. The emails were spoofed, but thousands of customers clicked on the link in the email and submitted the information at the webpage that opened up. On investigation, its found that the emails were sent by a disgruntled employee.
>
> **Case:** Thousands of employees of a global IT company ended up installing viruses on their computers when they executed an attachment appearing to have been sent out by their officers. The employees even disabled the anti-virus software because the email said that "the attachment may be incorrectly detected as a virus!" On investigation, it was found that the emails had been sent out by a rival company.

SMS spoofing is very similar to e-mail spoofing. The major difference being that instead of an email ID, a cell phone number is spoofed and instead of a spoofed e-mail, a spoofed SMS is sent.

> **Case:** A young lady received an SMS from her husband's cell phone informing her that he had had an accident and was at the hospital and urgently needed money. On receiving the SMS, she rushed out of the house with the

money. She was attacked and robbed by the person who had sent her the spoofed SMS.

An IP address (e.g. 75.125.232.93) is the primary identification of a computer connected to a network (e.g. the Internet). A criminal usually uses IP spoofing to bypass IP based authentication or to mislead investigators by leaving a trail of false evidence. IP spoofing can be accomplished using proxy servers and simple PHP scripts that are readily and freely available online.

> **Case:** Internet users in many countries use proxy servers to bypass Government imposed Internet censorship. (We are not passing any comment on whether is it right or wrong to impose Internet censorship or bypass it, as the case may be.)

> **Case:** A criminal hacked into the computer systems of a sensitive Government organization. The digital trail that he left behind led to a senior official of the same department. This officer would have been arrested immediately had it not been for his impeccable record. Detailed investigations proved that the digital trail was faked.

When you sit at a computer, open up a browser and type in www.asianlaws.org, you expect to reach the correct website (and most often you do!). This is because of the domain name system which converts human readable domain names such as asianlaws.org into computer readable IP addresses such as 75.125.232.93

DNS spoofing involves manipulating the domain name system to take unsuspecting victims to fake websites (that look identical to the original ones). Sitting at the computer you may type in www.asianlaws.org but the site that opens up may be a fake site!

This can and has been done at the local organizational level (e.g. by host file rewriting or by a network administrator with malicious intentions) or at the national or international level (by hackers exploiting vulnerabilities in the BIND software that runs most of the world's domain name servers).

> **Case:** Hundreds of employees at a global financial services company received emails from a popular online store about a huge discount on some popular books and DVDs. On clicking the link in the email, users were taken to what appeared to the website of the online store. Most of the recipients of the emails placed orders using their credit cards. No one got the books or the DVDs, all got was a hefty credit card bills at the end of the month.

On investigation it was uncovered that the network administrators had connived to carry out a simple Phishing attack. It was a fake email and a fake website. None of the victims (most of whom were advanced computer users) realized that something was amiss.

46. Piggy backing

It is the access to a wireless internet connection by bringing one's own computer within the range of another's wireless connection, and using that service without the subscriber's permission or knowledge.

It is a legally and ethically a controversial practice, with laws that vary in jurisdictions around the world.

Piggybacking is used as a means of hiding illegal activities, such as downloading child pornography or engaging in identity theft without leaving a trail of the piggybackers identity and thus leaving network owners subject to investigation for crimes of which are done through their networks.

A customer using the wifi service in a hotel or café provided by its owner, is generally not considered to be piggybacking, though non-customers or those outside the premises who are simply in reach may be called piggybackers.

Piggybacking is different from wardriving. Wardrivers collect information about the various unsecured wireless access

points (WAPs) they find while driving, without using the networks' services. Wardriving involves only the logging or mapping of the existence of access points whereas connecting to the network and using its services without authorization is referred to as piggybacking.

47. Piracy of Software

Unlike other things you purchase, the software you buy doesn't belong to you. Instead, you become a licensed user — you purchase the right to use the software on a single computer, but you can't put copies on other machines or pass that software along to others. Software piracy is the illegal distribution, unauthorized reproduction of software for business or personal use. Whether software piracy is deliberate or not, it is still illegal and punishable by law.

The roots of software piracy lie in the early 1960s, when computer programs were freely distributed with mainframe hardware by hardware manufacturers (e.g. AT&T, Chase Manhattan Bank, General Electric and General Motors). In the late 1960s, manufacturers began selling their software separately from the required hardware.

Software developers work hard to develop solid software programs. If those applications are pirated and stolen, the software developers will often be unable to generate the revenue thereby robbing the company of its fair share of profits. The effects of software piracy impact the entire global

economy. The reduced revenues often divert funding from product development, and result in less research and less investment in marketing. In 2007, economists indicated that software piracy cost the industry $39.6 billion.

Software piracy equals lost wages, lost jobs, and unfair competition. Struggling to fight against piracy, some companies must devote resources to anti-piracy technology, ultimately slowing down the development of better products and services. Others fail under the pressure of prices that legal resellers can't match.

Anti-copyright infringement organizations

Business Software Alliance (BSA)

Canadian Alliance Against Software Theft (CAAST)

Entertainment Software Association (ESA)

Federation Against Software Theft (FAST)

International Intellectual Property Alliance (IIPA)

Illustrations:

In 2008 eleven individuals were convicted in China for violating national copyright laws and participating in a sophisticated counterfeiting that enabled them to mass-produce and distribute pirated Microsoft software globally.

The group reportedly operated like an international corporation that produced and sold CDs and DVDs that were not only of high quality, but packaged nearly identically to real

products despite the high level of anti-piracy security measures taken by Microsoft.

The organization produced mass-pirated software such as Windows XP and Office 2007. The goods were sold via the Internet and then exported from China and shipped to the United States and Europe. The organization's international sales have been estimated at more than $2 billion.

In 2010 a 24-year-old Texas man Todd Alan Cook had been sentenced to 18 months in prison for selling more than US$1 million worth of pirated software online and pay $599,771 in restitution. He was guilty of criminal copyright infringement.

48. Pod Slurping

The act of using a portable data storage device such as an iPod, USB sticks, flash drives, PDAs and audio player to facilitate data theft is termed as pod slurping.

Illicit download of large quantities of sensitive and confidential data can be made by directly plugging the flash device into an organizations computer system.

As these storage devices are shrinking in size and growing in capacity, they are becoming an increasing security risk to companies and government agencies as they can be easily hidden.

Pod slurping is the latest weapon in the hacker's arsenal. And it's not only a method that sophisticated hackers can use but can be used by any amateur. All that is needed is the device, slurping software, and the opportunity to connect the device to the computer.

In 2004, security expert Abe Usher developed a program called “slurp.exe” that he used on his iPod to demonstrate how

information could easily be “slurped” from a computer. demonstration, it took just over a minute to download all files from the computer. This program makes it easier to search relevant directories on a computer system for typical business documents in Word and Excel format.

Illustration:

Golu an employee who's unhappy with his annual performance review and his lack of a pay hike decides to strike back by accessing the computer in the human resources desk. Using his iPod he slurps the excel sheet which stores all information about the companies employees.

49. Poisoning the Source

In this section, we will discuss a situation where a Trojan is implanted into a software product even before the product is released into the market!

Hackers can Trojanize software programs during the software's development and testing process. A hacker could join a software development company or contribute code to an open source software project.

As a developer or even a tester, the attacker could insert a relatively small backdoor of less than 100KB of code inside of hundreds of megabytes of legitimate code. This would be very difficult for anyone to detect.

Any users purchasing the product would then unwittingly be buying a Trojan embedded software and installing it on their systems..

Ken Thompson, noted UNIX co-creator and C programming language guru, discussed the importance of controlling source

code and the possibility of planting backdoors in it in his famous 1984 paper titled “Reflections on Trusting Trust,”

In that classic paper, Thompson described modifying the source code for a compiler so that it built a backdoor into all code that it compiles.

The proposed attack was particularly dangerous, as even a brand new compiler that is compiled with a Trojan version of the old compiler would have the backdoor in it.

In the words of Ken Thompson,

“You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code.

In demonstrating the possibility of this kind of attack, I picked on the C compiler. I could have picked on any program-handling program such as an assembler, a loader, or even hardware microcode. As the level of program gets lower, these bugs will be harder and harder to detect.

A well installed microcode bug will be almost impossible to detect”.

This concern is even more disturbing than the Trojanizing of software distribution sites that we discussed in the last section. When an attacker Trojanizes a software distribution site, the developers of the software at least have a clean version of the software that they can compare against to detect the deception.

Solving problems is relatively easier after discovery, as a clean version of the software can be placed on the website for distribution. On the other hand, if an attacker embeds a Trojan during the software development process, the vendor might not even have a clean copy. If the attackers are particularly clever, they will intertwine a small, inconspicuous backdoor throughout the normal code, making eradication extremely difficult.

A software developer would have to scan enormous quantities of code to ensure the integrity of a whole product. The larger the software product, the more difficult detection and eradication become.

Most modern software tools are vast in scope. Detecting bugs in code, let alone backdoors, is very difficult and costly. To Trojanize a software product, an evil employee doesn't even have to actually write an entire backdoor into the product.

Instead, the malicious developer could purposefully write code that contains an exploitable flaw, such as a buffer overflow, that would let an attacker take over the machine. Effectively, such a purposeful flaw acts just like a backdoor. If the flaw sneaks past the software testing team, the developer would be the only one who knows about the hole initially. By exploiting that flaw, the developer could control any systems using his or her code.

Various analyses and surveys have revealed that, on average, a typical developer accidentally introduces between 100 and 150 defects per 1,000 lines of code. Although these defects are entirely unintentional, a single intentional flaw could be sneaked in as well.

Although many of these errors are simple syntactical problems easily discovered by a compiler, many of the remaining defects often result in gaping security holes. In fact, in essence, a security vulnerability is really just the very controlled exploitation of a bug to achieve an attacker's specific goal.

If the attacker can make the program fail in a way that benefits the attacker (by crashing the system, yielding access, or displaying confidential information), the attacker wins. Estimating very conservatively, if only one in ten of the defects in software has security implications, that leaves between 10 and 15 security defects per 1,000 lines of code.

This looks even more dangerous when you consider that the Microsoft Windows XP operating system has approximately 45 million lines of code! Does this imply that Windows XP has about 450,000 security defects? Nobody knows for sure. What we do know is that the very same day that Windows XP was launched, Microsoft released megabytes of patches for it!

50. Pornography

There is no settled definition of pornography or obscenity. What is considered simply sexually explicit but not obscene in USA may well be considered obscene in India.

There have been many attempts to limit the availability of pornographic content on the Internet by governments and law enforcement bodies all around the world but with little effect.

Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories.

The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens.

Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression, it has been held that a law against obscenity is constitutional. The Supreme Court has defined obscene as “offensive to modesty or decency; lewd, filthy, repulsive.

Illustration:

December 2001 - A Fast Track Court sentenced Chennai-based orthopaedician Dr L Prakash to life imprisonment and three others to 7 years rigorous imprisonment in a cyber-porn case.

Prakash was arrested on charges of posting obscene pictures of women on the internet with the help of his brother in the US.

Illustration:

The Delhi Public School MMS Scandal is the sex scandal that involved the creation of pornographic MMS for 2.37 minutes by two 17 year old students of Delhi Public School and its illegal distribution as well as bid to auction it on Baazee.com.

Avnish Bajaj, the then CEO of the website Baazee.com was summoned by the Delhi High Court for having allowed this clip to be listed for auction on is site. However, the two students from the clip were not prosecuted since they were minors.

51. robots.txt file

A robot is a program that automatically traverses the Internet by visiting a web page and then retrieving all linked files.

Web robots are sometimes referred to as Web Wanderers, Web Crawlers, or Spiders. These names are a bit misleading as they give the impression that the software itself moves between sites like a virus.

This is not the case. A robot simply visits sites by requesting documents from them.

To see a list of active robots and their features, visit: http://www.robotstxt.org/wc/active.html

The quick way to prevent all robots from visiting a website is to put these two lines into the robots.txt file on the server:

User-agent: *

Disallow: /

Illustration

User-agent: webcrawler

Disallow: /tmp

Disallow: /logs

This indicates that the robot called webcrawler should not visit URLs starting with /tmp or /log.

A webmaster would usually create the robots.txt file in such a way that robots do not visit the portions of the website that contain sensitive information. A hacker can examine the robots.txt file and get an indication of which parts of the website he should target.

52. Port scanning

Port has a dual definition in computers. There are many different ports on the computer itself: ports to plug in a mouse, keyboard, USB devices, printer, monitor, etc.

However, the types of ports that are more relevant to information security are the virtual ports found in Transmission Control Protocol / Internet Protocol (TCP/IP). TCP/IP is the basic communication language or protocol of the Internet.

Ports are like channels on your computer. Normal web or http (hyper text transfer protocol) traffic flows on port 80. POP3 (Post Office Protocol) email flows through port 110. By blocking or opening these ports into and out of your network you can control what kind of data can flow through your network.

Scanning a port can be compared with a security guard traversing a neighborhood and checking every door and window to assess which doors or windows are open and which are locked.

Port Scanning is the act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open “doors” to a computer. Port scanning has legitimate uses such as in managing networks, but can also be malicious in nature if someone is looking for a weakened access point to break into a computer.

Port scanning is also a prominent technique used to reveal what services are available (in order to plan an exploit involving those services), and to determine the operating system of a particular computer. A program that attempts to learn about the weaknesses of a computer or network edge device by repeatedly probing it with requests for information can be called a port scanner.

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two of the protocols that make up the TCP/IP protocol suite which is used universally to communicate on the Internet. Each of these has ports 0 through 65535 available so essentially there are more than 65,000 “doors” to a computer.

The first 1024 TCP ports are called the Well-Known Ports and are associated with standard services such as, HTTP, FTP (File Transfer Protocol) SMTP (Simple Mail Transfer Protocol) or DNS (Domain Name System).

Some of the addresses over 1023 also have commonly associated services, but the majority of these ports are not associated with any service and are available for a program or application to use to communicate on.

For a detailed listing of port numbers please visit: http://www.iana.org/assignments/port-numbers

If a port scan is being conducted with malicious intent, the intruder would generally prefer to go undetected. Network security applications can be configured to alert administrators if they detect connection requests across a broad range of ports from a single host.

To get past this problem, intruders can scan the ports in strobe or stealth mode.

Strobing limits the ports to a smaller target set rather than blanket scanning of all 65536 ports. Stealth scanning utilizes techniques such as reducing the speed of the scan. By scanning the ports over a much longer period of time the chance that the target will sound an alarm also goes down.

There are a number of different methods to perform the actual port scans as well as tricks to hide the true source of a port scan.

53. Rootkits

A cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network.

A rootkit may consist of spyware and other programs that monitor traffic and keystrokes; create a backdoor into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection.

Rootkit detection is difficult because a rootkit may be able to demolish the software that is intended to find it. Removal can be complicated or practically impossible. Reinstallation of the operating system may be the only available solution to the problem. When dealing with firmware rootkits, removal may require hardware replacement, or specialised equipment.

54. Salami Theft

These attacks are used for committing financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed.

For instance, a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 2 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.

Why this attack is called a "salami attack"? Some security specialists claim that it refers to slicing the data thinly, like salami. Others argue that it means building up a significant object or amount from tiny scraps, like salami.

Illustration:

In January 1993, four executives of a rental-car franchise in Florida USA were charged with defrauding at least 47,000 customers using a salami technique.

They modified a computer billing program to add five extra gallons to the actual gas tank capacity of their vehicles. From 1988 through 1991, every customer who returned a car without topping it off ended up paying inflated rates for an inflated total of gasoline. The thefts ranged from $2 to $15 per customer - difficult for the victims to detect.

Illustration:

In January 1997, Willis Robinson of Maryland USA, was sentenced to 10 years in prison (six of which were suspended) for having reprogrammed his Taco Bell drive-up-window cash register - causing it to ring up each $2.99 item internally as a 1-cent item, so that he could pocket $2.98 each time.

He made $3,600 before he was caught. Another correspondent adds that management assumed the error was hardware or software and only caught the perpetrator when he bragged about his crime to co-workers.

Illustration:

In Los Angeles USA in October 1998, four men were charged with fraud for allegedly installing computer chips in gasoline pumps that cheated consumers by overstating the amounts pumped.

The problem came to light when an increasing number of consumers claimed that they had been sold more gasoline than the capacity of their gas tanks.

However, the fraud was difficult to prove initially because the perpetrators programmed the chips to deliver exactly the right amount of gasoline when asked for five- and 10-gallon amounts - precisely the amounts typically used by inspectors.

Illustration:

Teja a criminal uses the banks computer to transfer twenty or thirty cents at a time from various customers and divert it to his own dummy account.

He does not divert money more than 3 times a year from a particular customer. A customer does not notice such a small discrepancy in his monthly bank statement and even if he would have noticed it he would not use his effort and time by going to bank for this.

Illustration:

Mr. Sonawalla a banker at Holu-Holu Bank used to round off any sum ending in fractions to the nearest whole number in the customer's monthly statement.

He created a dummy account at his own bank and he programs the computer to divert the money from the round offs to his account. This turned to a handsome amount over the years.

55. Sale of Illegal Articles

It is becoming increasingly common to find cases where sale of illegal articles such as narcotics drugs, weapons, wildlife etc. is being facilitated by the Internet. Information about the availability of the products for sale is being posted on auction websites, bulletin boards etc.

It is practically impossible to control or prevent a criminal from setting up a website to transact in illegal articles. Additionally, there are several online payment gateways that can transfer money around the world at the click of a button.

The Internet has also created a marketplace for the sale of unapproved drugs, prescription drugs dispensed without a valid prescription, or products marketed with fraudulent health claims.

Many sites focus on selling prescription drugs and are referred to by some as "Internet pharmacies." These sites offer for sale either approved prescription drug products, or in some cases, unapproved, illegal versions of prescription drugs. This poses a serious potential threat to the health and safety of patients.

The broad reach, relative anonymity, and ease of creating new or removing old websites, poses great challenges for law enforcement officials.

Illustration:

In March 2007, the Pune rural police cracked down on an illegal rave party and arrested hundreds of illegal drug users. The social networking site Orkut.com is believed to be one of the modes of communication for gathering people for the illegal "drug" party.

56. Scavenging

Scavenging is also known as dumpster *diving*. Scavenging is looking for treasure in someone else's trash.

It isn't limited to searching through the trash for obvious treasures like access codes or passwords thrown away, but also thrown away trash sensitive information containing addresses, phone numbers, credit card receipts, social security number, calendar or organizational chart. Such data can be used to assist an attacker using social engineering techniques to gain access to a computer network or cause any kind of theft or fraud.

Illustrations:

In 2010 William T. Frelix and 11 others were indicted on charges that they used other people's identities and credit card numbers to pay for more than $100,000 in goods and services. Frelix was the ringleader of the theft and credit card scam in which he directed others to go fishing in hotel and motel Dumpsters for other people's credit card information.

57. Smishing

This is morphology of SMS and phishing – SmiShing. It is the same as "phishing," in which you receive an email that seems to be from a reputable source, asking for your credit card data, password, or other private information. Only instead of an email, smishing takes place through the SMS text messages you receive on your cell phone.

Illustration:

Kunal gets a message on his phone asking him to click on a link to get sleazy pictures of Bollywood and Hollywood actresses. He clicks on the link and is directed to a web page wow.com where there pictures of animals doing funny things. Within the next 10 minutes Kunals phone crashes.

Illustration:

Joey gets a message on his phone telling him that he has won Rs. 500 extra balance in his mobile service providers lucky draw contest and to get the same he should send a message 'get balance' to a particular number. After sending the message Joey realizes instead of getting balance he loses all his balance and is left with no money on his phone.

58. Social Engineering

In the realm of computers, it is a non-technical technique- the act of obtaining or attempting to obtain secure data by deceiving individuals into revealing secure information is social engineering.

It is the art of psychologically manipulating victims of social engineering into performing actions or revealing confidential information without realizing it's a fraud. In most cases the attacker never comes face-to-face with the victims.

They rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it.

A social engineer runs what is to be called a con game. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. Social engineering techniques appeal to the victims' kindness, appeal to vanity, appeal to authority, appeal to greed, and old-fashioned eavesdropping.

Illustrations:

A caller contacted AOL's tech support and spoke with an employee for an hour. During the conversation the caller mentioned that his car was for sale at a great price.

The employee was interested, so the caller sent an e-mail attachment with a picture of the car. Instead of a car photo, the mail executed a backdoor exploit that opened a connection out from AOL through the firewall.

Through this combination of social engineering and technical exploitation, the caller gained access to the internal network of AOL thus the attack that compromised their system and revealed confidential information of more than 200 accounts.

Illustrations:

March 2011: Malware using social engineering tricks was sent to people by appealing to their empathy. Scammers were spreading malicious links to "dramatic" videos of the Japan Earthquake disaster. When a person searched for news on the earthquake or tsunami they ended up clicking on a link that actually downloaded malware onto their PC.

In addition to sending spam emails and poisoning search results with dangerous links, cybercrooks also posted donation requests and links containing malware on social networking sites. Therefore money, credit card, as well as identity information, would be stolen.

59. Spambot

A spambot is an automated computer program designed to send unsolicited bulk messages indiscriminately.

They harvest e-mail addresses from material found on the Internet by automatically "crawling" the web, newsgroups, chat rooms, instant messengers and other contact databases to locate any and every email address they can find in order to build mailing lists for sending these e-mail, also known as spam.

They usually create fake accounts and send spam using them, whereas some spambots can crack passwords and send spam using other people's accounts.

In the year 2011, the estimated figure for spam messages was around seven trillion.

There are various types of Spambots like:

Spam: is unsolicited bulk messages sent over email.

Spim: is sending spam over instant messenger.

Spat: is sending spam over internet telephony.

Spyware:

The term spyware is a type of malware software that is installed on a personal computer without the user's informed consent and is typically hidden from the user hence can be difficult to detect.

Spyware programs monitor the user's activities. It can also collect various types of personal information, almost any type of data, including Internet surfing habits, user logins, bank or credit account information and sites that have been visited.

They also interfere with user control of the computer such as installing additional software, redirecting Web browser activity or accessing websites blindly that will cause more harmful viruses to be installed.

Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other program.

Illustration:

Movieland, also known as Moviepass.tv and Popcorn.net, is a movie download service that has been the subject of thousands of complaints to the Federal Trade Commission (FTC) and other agencies.

Consumers complained they were held hostage by a cycle of oversized pop-up windows demanding payment of at least

$29.95, claiming that they had signed up for a three-day free trial but had not cancelled before the trial period was over, and were thus obligated to pay.

The FTC filed a complaint, against Movieland and other defendants charging them with having "engaged in a nationwide scheme to use deception and coercion to extract payments from consumers."

CoolWebSearch is a group of programs that has the ability to exploit the weaknesses of Internet Explorer. This spyware can manipulate direct traffic to advertisements on coolwebsearch.com. Displaying pop-up ads, it manipulates search engine results, and alters your computer's host files to direct DNS lookups to these sites.

60. SQL Injection

SQL injection is one of the many web attack techniques used by hackers to steal data from databases through a website.

It takes advantage of improper coding of web applications that allows the hacker to inject SQL commands into one's site to allow them to gain access to the data held within the database.

This is done by including portions of SQL statements in a web form entry field to get the website to pass a newly formed rogue SQL command to the database (e.g. dump the database contents to the attacker).

SQL injection is a code injection technique that exploits a security vulnerability in a website's software.

Illustration :

June 2011, Lady Gaga's website was hacked by a group of US cyber attackers called SwagSec and thousands of her fans' personal details were stolen from her website.

The hackers took a content database dump from www.ladygaga.co.uk and a section of email, first name, and last name records were accessed.

An SQL injection vulnerability for her website was recently posted on a hacker forum website, where a user revealed the vulnerability to the rest of the hacker community.

While no financial records were compromised, the blog implies that Lady Gaga fans are most likely receiving fraudulent email messages offering exclusive Lady Gaga merchandise, which contained malware.

August 2009, an American citizen Albert Gonzalez and two unnamed Russians were charged with the theft of 130 million credit card numbers using an SQL injection attack.

In reportedly "the biggest case of identity theft in American history", they stole cards from a number of corporate victims after researching their payment processing systems.

Among the companies hit were credit card processor Heartland Payment Systems, convenience store chain 7-Eleven, and supermarket chain Hannaford Brothers.

61. Stealware

Stealware is software that modifies affiliate tracking codes by replacing their affiliate cookies on a user's computer or by overlaying links on a web site with another affiliates tracking link. As a result of this commissions are directed to the owner of the stealware instead of the owner of the site.

Therefore it is a type of software that effectively transfers money owed to a website owner to a third party.

Illustration

A develops a site that generates a modest revenue from cost per action (CPA or affiliate) referrals to other sites.

Its effort is to get the traffic, the visitors to the site follow links you have set up to other sites and purchase things, for which it receives a referral fee. B resets the tracking codes to their own in order skim off payouts due to A.

This is Stealware.

62. Time Bomb

A time bomb program or batch file waits for a specific time before causing damage. Therefore a time bomb detonates when the clock of the computer reaches a preset date where it will cause the computer to crash or release a virus, worm or Trojan on such a date. Time bombs are a type of logic bomb.

In computer software, a time bomb refers to a computer program that has been written so that it will stop functioning after a predetermined date or time is reached

Time-bombs are often used by disgruntled and dishonest employees who find out they are about to be fired or by dishonest consultants who put unauthorized time-outs into their programs without notifying their clients.

Illustrations:

The Michelangelo virus of 1992 was designed to damage hard disk directories on the 6th of March every year

Illustrations:

The infamous Jerusalem virus (also known as the Friday the 13th virus) of 1988 was a time bomb. It duplicated itself every Friday and on the 13th of the month, causing system slowdown; however, on every Friday the 13th after May 13, 1988, it also corrupted all available disks on the infected systems

63. Trojan

In the 12th century BC, Greece declared war on the city of Troy. The dispute was caused due to the fact that the prince of Troy and the Queen of Sparta eloped. Hence declaring that they intend to marry.

The Greeks besieged Troy for 10 years but met with no success as Troy was very well fortified.

In a last effort, the Greek army pretended to be retreating, and left behind a huge wooden horse. The people of Troy saw the horse and thought it was a gift from the Greeks.

They pulled the horse into their city, unaware that the hollow wooden horse had some of the best Greek soldiers hiding inside it.

Under the cover of night, the soldiers snuck out and opened the gates of the city, and later, together with the rest of the army, besieged and destroyed Troy.

Similar to the wooden horse, a Computer Trojan (also referred to as Trojan Horse program) pretends to do one thing while actually doing something completely different.

This chapter is based upon excerpts from writings of Ed Skoudis provided courtesy of Addison Wesley Professional.

A Trojan Horse program is a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality.

Today's Trojan horses try to sneak past computer security fortifications (such as firewalls), by employing like-minded trickery. By looking like normal software, Trojan horse programs are used for the following goals:

• Duping a user or system administrator into installing the Trojan horse in the first place. In this case, the Trojan horse and the unsuspecting user becomes the entry vehicle for the malicious software on the system.

• Blending in with the "normal" programs running on a machine. The Trojan horse camouflages itself to appear to belong on the system so users and administrators continue their activity, unaware of the malicious code's presence.

Attackers have devised a myriad of methods for hiding malicious capabilities inside their wares on your computer. These techniques include

• employing simple, yet highly effective naming games,

• using executable wrappers,

• attacking software distribution sites,

• manipulating source code,

• co-opting software installed on your system, and

• disguising items using polymorphic coding techniques.

As we discuss each of these elements, we must bear in mind that the attackers' main goal is to disguise the malicious code so that the victims do not realize what the attacker is up to.

Types of Trojans

The most common types of Trojans found today are:

1. Remote Administration Trojans (RATs)

These are the most popular Trojans. They let a hacker access the victim's hard disk, and also perform many functions on his computer (shut down his computer, open and shut his CD-ROM drive etc.).

Modern RATs are very simple to use. They come packaged with two files - the server file and the client file. The hacker tricks someone into running the server file, gets his IP address and gets full control over the victim computer.

Some Trojans are limited by their functions, but more functions also mean larger server files. Some Trojans are merely meant for the attacker to use them to upload another Trojan to the target's computer and run it; hence they take very little disk space. Hackers also bind Trojans into other programs, which

appear to be legitimate, e.g. a RAT could be bound with an e-greeting card.

Most RATs are used for malicious purposes - to irritate or scare people or harm computers. There are many programs that detect common Trojans. Firewalls and anti-virus software can be useful in tracing RATs.

RATs open a port on your computer and bind themselves to it (make the server file listen to incoming connections and data going through these ports). Then, once someone runs his client program and enters the victim's IP address, the Trojan starts receiving commands from the attacker and runs them on the victim's computer.

Some Trojans let the hacker change this port into any other port and also put a password so only the person who infects the specific computer will be able to use the Trojan. In some cases the creator of the Trojan would also put a backdoor within the server file itself so he'll be able to access any computer running his Trojan without the need to enter a password.

This is called "a backdoor within a backdoor" e.g. CIA, Netbus, Back Orifice, Sub7.

2. Password Trojans

Password Trojans search the victim's computer for passwords and then send them to the attacker or the author of the Trojan. Whether it's an Internet password or an email password there is a Trojan for every password. These Trojans usually send the information back to the attacker via email.

3. Privileges-Elevating Trojans

These Trojans are usually used to fool system administrators. They can either be bound into a common system utility or pretend to be something harmless and even quite useful and appealing. Once the administrator runs it, the Trojan will give the attacker more privileges on the system. These Trojans can also be sent to less-privileged users and give the attacker access to their account.

4. Key loggers

These Trojans are very simple. They log all of the victim's keystrokes on the keyboard (including passwords), and then either save them on a file or email them to the attacker once in a while. Key loggers usually don't take much disk space and can masquerade as important utilities, thus becoming very hard to detect.

5. Joke Programs

Joke programs are not harmful. They can either pretend to be formatting your hard drive, sending all of your passwords to some hacker, turning in all information about illegal and pirated software you might have on your computer to the police etc. In reality, these programs do not do anything.

6. Destructive Trojans

These Trojans can destroy the victim's entire hard drive, encrypt or just scramble important files. Some might seem like joke programs, while they are actually destroying every file they encounter.

In an unreported case in India, a Trojan almost led to the death of a reporter!

A young lady was working on an article about 'online relationships'. During the course of researching for the article, she befriended many strangers online. One of these people remotely implanted a Trojan on her home computer.

Staying in a small one-bedroom apartment in Mumbai, her computer was in one corner. Unknown to her, the Trojan had hijacked her web-camera and her microphone, both of which were attached to her computer.

Numerous pictures of her in compromising positions were hijacked by the hacker who then uploaded them on to a pornographic website. When the young lady came to know about it a year later, she attempted suicide. Fortunately she survived.

This is a shocking reminder of the disastrous effects that a Trojan can have.

This section discusses two cases where Trojans had been used to frame innocent persons for having committed serious crimes.

1. UK child porn case

A British citizen, Julian Green, was arrested in October 2002 after the police raided his home and found 172 indecent pictures of children on the hard disk of his home computer.

Green was an IT contractor in the UK defence industry. He was a divorcee with two children.

As a result of 13 paedophile related charges brought against him, he lost his job, was attacked and was unable to see his children.

Under British law the maximum sentence for possession of such images is ten years' imprisonment, and anyone convicted in such a matter would have become subject to registration with the police as a sex offender for a period of five years.

Green claimed that the pictures found on his computer had nothing to do with him and that he had no interest in pedophilia and had no pornographic magazines or videos at his home. He had no history of sexual offences and was an honest man trusted with a sensitive job that required security clearance.

An extensive examination of Green's computer hard disk showed the presence of 11 Trojan horse programs. These Trojans were set to log onto "inappropriate sites" without Green's permission whenever he accessed the Internet. These Trojans were believed to have come from unsolicited emails that Green opened before he deleted them.

The charges against him were finally dropped on account of the discovery of these Trojans on his computer.

In previous instances, the prosecution had been able to show that the Trojan defense was implausible. On behalf of the police, computer experts have been able to show that pictures were viewed and moved around the computer; that they did

not appear in the locations that would indicate pop-ups; that there was no remaining indication of the spam email; and no evidence of any Trojan application.

Armed with this weight of evidence, courts have had no problem in dismissing the Trojan defense in other cases.

In this case, though, it was certain that there was evidence: the Trojan was indeed found and it was discovered that it referred to the pedophile pictures explicitly.

Experts were able to show that the defendant had not accessed the pictures and that he could not have known they were on his computer.

This final point is important. The actual offence under which most charges of computer pedophilia are brought is UK's 1988 Criminal Justice Act. Section 160 makes it an offence to be in possession of an indecent photograph of a child.

In this case there was no dispute about the fact that the pictures were indeed on his computer and were indeed indecent photographs of children.

There are, however, three defenses: that the picture was in his possession for a legitimate reason; that he had not seen the picture or had any reason to believe it was indecent; and that it was unsolicited and not kept for any length of time.

The first defense is the one that gives permission for experts working on behalf of the courts to possess the pictures in the course of their investigations.

The second and third defenses were claimed in this case: the pictures were not solicited and were not viewed. The third defense also provides protection for those increasingly common situations in which extreme material - including pedophile content - is being transmitted in spam.

2. The Texas port DoS case

Aaron Caffrey, a 19 year old UK citizen, was accused of crashing systems at the port of Houston in Texas, USA. He faced a charge of unauthorized modification of computer material at a UK court.

During the trial, it was claimed Caffrey had perpetrated a complex crime, involving computer hacking, identity theft and fraudulent financial-market trading.

The prosecutor in the case claimed that Caffrey hacked into the computer server at the port in order to target a female chatroom user called Bokkie, following an argument. It was said in court that they had argued over anti-US remarks she had made.

Caffrey, who suffers from a form of autism called Asperger's Syndrome, was said to be in love with an American girl called Jessica. The court was told he named his computer after her and dedicated his "attack script" to her. Scheduling computer systems, at the port, were bombarded with thousands of electronic messages on 20 September, 2001.

The attack froze the port's web service, which contained vital data for shipping, mooring companies and support firms responsible for helping ships navigate in and out of the harbor.

An investigation by US authorities traced the computer's IP address to a computer at Caffrey's home. But the teenager claimed an unidentified third party had planted the instructions for the attack script on his website without his knowledge.

He also criticized the authorities for not uncovering the virus during their investigation. On the final day of the trial, Caffrey admitted being part of a group of hackers called Allied Haxor Elite, but denied he had ever illegally hacked into a computer.

The teenager told the court that hackers operated legally, but that people who entered computer systems illegally were known as "crackers". He said: "I have hacked into computers legally for friends to test their server security because they asked me to but never illegally."

Caffrey was found not guilty of computer crime after the jury accepted his story that attackers used an unspecified Trojan to gain control of his PC and launch the assault. The prosecution argued that no trace of Trojan infection was found on Caffrey's PC but the defense was able to counter this argument with testimony from Caffrey that it was possible for a Trojan to delete itself.

Illustration:

In May 2002, Monkey.org, a website that distributes popular security and hacking tools, was hacked into.

The hackers modified the following tools distributed through Monkey.org:

1. The Dsniff sniffing program,

2. The Fragroute IDS evasion tool and

3. The Fragrouter IDS evasion tool.

The hackers replaced each tool with a Trojan horse version that created a backdoor on the systems of anyone who downloaded and installed these tools.

This attack was especially lethal as these tools are widely used by security professionals as well as by hackers.

Illustration:

From July 30 to August 1, 2002, an attacker loaded a Trojan horse version of the Open Secure Shell (OpenSSH) security tool onto the main OpenSSH distribution Website (OpenSSH is widely used to provide tight security for remote access to a system).

However, diligent administrators who tried to protect their systems by downloading this security tool in late July 2002, unwittingly installed a backdoor.

Illustration:

From September 28 until October 6, 2002, a period of more than one week, the distribution point for the most popular e-mail server software on the Internet was subverted.

The main FTP server that distributed the free, open source Sendmail program was Trojanized with a backdoor.

Illustration:

From November 11 to 13, 2002, tcpdump, the popular sniffing program, and libpcap, its library of packet capture routines, were replaced with a Trojan horse backdoor on the main tcpdump website.

Not only is the tcpdump sniffer widely used by security, network, and system administrators around the world, but the libpcap (pronounced lib-pee-cap, which is short for "library for packet capture") component is a building block for numerous other tools.

Administrators who installed tcpdump, libpcap, or any other package built on top of libpcap during this time frame were faced with a backdoor running on their systems.

64. URL Manipulation

URL is a short form to Uniform Resource Locator - it is a web address of a web page.

URL manipulation can be employed as a convenience by a Web server administrator or for evil purposes by a hacker. Malicious URL manipulation is when the user requests are redirected from a legitimate site to an illegitimate or bogus site which may then install rogue code on the user's hard drive.

Using URL to commit an internet scam is pretty common nowadays owing to simplicity in manipulation and easy spreading around.

URL manipulation is dangerous when it leads to a phishing site. Phishing site is always the best place to land the URL because it does not look suspicious at all at the first glance because the graphical user interface always look like the original one. If you do not check the URL, it is very hard for you to differentiate between the actual site and the phishing site.

Illustrations:

URL manipulation flaw was exploited back in 2010 on the AT&T website to extract email addresses and other information about iPad owners. The two hackers involved are currently facing criminal charges for carrying out that attack.

Hackers stole information of 200,000 Citi credit card holders by exploiting a simple flaw in the company's Citi Account Online system. The customer information URL contained the account numbers as a parameter to access the site and simply changing the value revealed details about other account holders.

The hackers created a script that tried possible account numbers and saved the data corresponding to those that actually existed. Using this method they managed to successfully extract the names, account numbers and contact information for about 1% of Citigroup's North American customers, until the company discovered the attack during a routine check.

65. Virus Attack

A computer virus is a man made program or piece of code that is loaded onto one's computer without the victims' knowledge and runs against his/her wishes.

Viruses can also replicate themselves over and over again and is relatively easy to produce. Even a simple virus is dangerous because it corrupts the system.

An even more dangerous type of virus is the one capable of transmitting itself across networks and bypassing security systems.

Viruses can be transmitted as attachments to an e-mail note or in a downloaded file, or be present on a diskette or CD.

The sender of the e-mail note, downloaded file, or diskette you've received is usually unaware that it contains a virus. Some viruses wreak havok as soon as their code is executed while other viruses lie dormant until circumstances cause their code to be executed by the computer.

E-mail viruses: An e-mail virus travels as an attachment to e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book. Some e-mail viruses don't even require a double-click they launch when you view the infected message in the preview pane of your e-mail software

The different damages a virus can cause:

- An annoying message appearing on the computer screen.
- Reduce memory or disk space.
- Modify existing data.
- Overwrite or Damage files.
- Erase hard drive.

Illustration:

Back in March 1999, the Melissa virus was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could be contained.

Illustration:

Chernobyl or Spacefiller, is a Microsoft Windows computer virus written in Taiwan. It is one of the most damaging viruses, overwriting critical information on infected system drives, and more importantly, in some cases corrupting the system BIOS (basic input output system).The name "Chernobyl Virus" was

coined some time after the virus was already well known as CIH, and refers to the complete coincidence of the trigger date of the virus and the nuclear disaster which occurred in Chernobyl, Ukrainian SSR on April 26, 1986.

66. Web defacement

Website defacement is usually the substitution of the original home page of a website with another page (usually pornographic or defamatory in nature) by a hacker.

Religious and government sites are regularly targeted by hackers in order to display political or religious beliefs. Disturbing images and offensive phrases might be displayed in the process, as well as a signature of sorts, to show who was responsible for the defacement.

Websites are not only defaced for political reasons, many defacers do it just for the thrill. For example, there are online contests in which hackers are awarded points for defacing the largest number of web sites in a specified amount of time.

Corporations are also targeted more often than other sites on the Internet and they often seek to take measures to protect themselves from defacement or hacking in general.

Web sites represent the image of a company or organisation and these are therefore especially vulnerable to defacement.

Visitors may lose faith in sites that cannot promise security and will become wary of performing online transactions. After defacement, sites have to be shut down for repairs, sometimes for an extended period of time, causing expenses and loss of profit.

Illustration:

Mahesh Mhatre and Anand Khare (alias Dr Neukar) were arrested in 2002 for allegedly defacing the website of the Mumbai Cyber Crime Cell.

They had allegedly used password cracking software to crack the FTP password for the police website. They then replaced the homepage of the website with pornographic content. The duo was also charged with credit card fraud for using 225 credit card numbers, mostly belonging to American citizens.

Illustration:

In 2001, over 200 Indian websites were hacked into and defaced. The hackers put in words like bugz, death symbol, Paki-king and allahhuakbar.

In the case of 123medicinindia.com, a message was left behind which said

"Catch me if uuu can my deraz lazy adminzzz"

challenging the system administrators to trace the miscreants.

The offenders were allegedly a group of hackers who go by the name of 'Pakistani Cyber Warriors'.

Illustration:

In 2006, a Turkish hacker using the handle iSKORPiTX was able to breach the security of a group of web servers, containing more than 38,500 web sites in less than a day!

Illustration:

The first Defacers Challenge took place on Sunday, July 6, 2003. There was a special prize for the first contestant to deface 6,000 web sites.

The contest was conducted over a six-hour period. Points were awarded based on the server's operating system.

Windows: 1 point,

Linux: 2 points,

BSD: 2 points,

AIX: 3 points,

HP-UX: 5 points

Macintosh: 5 points

67. Vishing

With the growth of mobile banking and the ability to conduct financial transactions online, vishing attacks have become even more attractive and lucrative for cyber criminals. It is the telephone equivalent of phishing.

The term is a combination of “voice” and phishing. Vishing is the criminal act of using voice email, VoIP (voice over Internet Protocol), landline or cellular telephone to gain access to private, personal and financial information from the public for the purpose of financial reward by committing identity theft. It is typically used to steal credit card numbers by a scammer who usually pretends to be in legitimate business, and fools the victim into thinking he or she will profit.

Vishing is very hard for legal authorities to monitor or trace. Thus it is onto the consumers to protect themselves, by being highly suspicious when receiving messages directing them to call and provide credit card or bank numbers. When in doubt, calling a company's telephone number listed on billing statements or other official sources is recommended instead of calling numbers from messages of dubious authenticity.

68. Wire - Tapping

Wire tapping is the monitoring of telephone and Internet conversations by a third party, often by secret means.

It is a form of electronic eavesdropping on data or voice transmissions by attaching unauthorized equipment or overhearing communications by means of a concealed recording or listening device or by intercepting and interpreting broadcast data in the case of wireless phones, cellular phones, and wireless networks.

Wiretapping therefore is a particular form of Electronic Surveillance that monitors telephonic and telegraphic communication.

Illustration:

In the Greek telephone tapping case 2004-2005 more than 100 mobile phone numbers belonging mostly to members of the Greek government, including the Prime Minister of Greece, and top-ranking civil servants were found to have been illegally tapped for a period of at least one year.

The Greek government concluded this had been done by a foreign intelligence agency, for security reasons related to the 2004 Olympic Games, by unlawfully activating the lawful interception subsystem of the Vodafone Greece mobile network.

Illustration:

The 'Radia tapes controversy' relates to the discussion between Nira Radia and various politicians, corporates and industrialists, officials, bureaucrats, aides and journalists that were taped by the Indian Income Tax Department in 2008–09.

The tapes led to government and public accusation that these calls evidence the planning of the 2G spectrum scam and other criminal and unconstitutional activities.

69. Worm

Computer worms are standalone malware programs that will use your computer network to replicate themselves in order to spread to other computers. Unlike a computer virus, it does not need to attach itself to any program, file or document.

In some ways worms are more deadly than viruses because they don't need to lodge themselves into programs to replicate – worms can replicate independently through your system.

Once in your system, worms will look scan your network for other machines that may have similar security holes. If the worm finds one, it will copy itself into the new computer and start the process all over again.

Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

Worms can perform a variety of operations according to how it has been designed.

- It can cause a denial of service attack
- It gets attached to Microsoft outlook or any such mailing facility and sends mails to everybody on the address list (replicates itself and passes on the worm to everyone in the address list),
- overwrites your files and documents, and
- Makes your computer slow and dysfunctional.

Illustration:

Nuwar OL is a worm received through email with subjects like "You Are In My Dreams," "I Love You So Much," "Inside My Heart Is You," etc. The mail consists of a website link, which downloads the malicious worm when accessed.

To disguises its activity, the worm redirects you to a web page with the theme of a romantic greeting card. Once the computer is infected, the infection spreads by sending messages to names in the user's address book. The most severe impact of the Nuwar OL is slowing down the performance of a single computer or a network.

Illustration:

The ILOVEYOU virus comes in an e-mail note with "I LOVE YOU" in the subject line and contains an attachment that, when opened, results in the message being re-sent to everyone in the

recipient's Microsoft Outlook address book and, perhaps more seriously, the loss of every JPEG, MP3, and certain other files on the recipient's hard disk.

As Microsoft Outlook is widely installed as the e-mail handler in corporate networks, the ILOVEYOU virus can spread rapidly from user to user within a corporation. On May 4, 2000, the virus spread so quickly that e-mail had to be shut down in a number of major enterprises such as the Ford Motor Company. The virus reached an estimated 45 million users in a single day.

Illustration:

Code Red was a computer worm observed on the Internet on July 13, 2001. It attacked computers running Microsoft's IIS web server. The worm was named the "Code Red" worm because Code Red Mountain Dew was what the researches were drinking after discovering the virus.

The phrase "Hacked by Chinese!" was the phrase with which the worm defaced websites. Although the worm had been released on July 13, the largest group of infected computers was seen on July 19, 2001, the number of infected hosts reached 359,000. The worm spread itself using a common type of vulnerability known as a buffer overflow.

70. XSS Attack

An abbreviation of cross-site scripting, Cross-Site Scripting attacks is a method in which malicious scripts are injected into an otherwise trusted web site. An attacker can use XSS to send a malicious script to an unsuspecting user.

The user's browser has no way to know that the script should not be trusted, and will execute the script since it thinks the script came from a trusted source.

By injecting malicious scripts into web pages, an attacker can gain access to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user.

Cross-site scripting carried out on websites accounted for roughly 80.5% of all security vulnerabilities documented by Symantec as of 2007. Their effect may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site.

Illustration:

In Shasha's website there is a comment tab for the photographs in the photo album. He created a feature that lets his viewers comment on his photos by submitting the comment and he does not have much validation in this comment tab.

Now Gogo (an intruder) visits Shasha's website and he's jealous of Sasha's website traffic and wants to steal some of his website. So he inserts the following code to his comment tab

Hi Sasha, very gud job, keep it up!

And every time a user visits Sasha's photos, they are redirected to Gogo's site.

71. Zero Day Attack

A zero day attack, also known as a zero hour attack, takes advantage of a previously unknown computer vulnerability that does not currently have a solution.

Zero-day attacks are used by attackers before the developer of the target software knows about the vulnerability. Since the vulnerability isn't known in advance, there is no way to guard against the exploit before it happens.

Also a software company in some cases would have discovered the problem in the software after it has been released and will offer a patch or update or fix it but before it does so the attacker will take advantage of that problem.

By finding software vulnerabilities before the software's makers find them or solve them, a programmer can create a virus or worm that exploits that vulnerabilities and harms computer systems in a variety of ways.

A zero day attack can be harmful to specific computers long after the patch has been created and the vulnerability has been closed. This is because many computer owners do not regularly update their software with patches made available by the software makers.

Illustration:

On November 09, 2006, there was a zero-day attack on a part of Windows called the XMLHTTP 4.0 ActiveX Control. When a web browser opened an infected web page in Internet Explorer (IE), it called the ActiveX control, which then helped the attacker to cause a buffer overflow. Attackers were then able to download Spyware and steal data of the users.

Illustration:

Adobe issued an alert in 2010 to warn about zero-day attacks against an unpatched vulnerability in its Reader and Flash Player software products. The vulnerability, described as critical, affects Adobe Flash Player 10.0.45.2 and earlier versions for Windows, Macintosh, Linux and Solaris operating systems.

It also affects the authplay.dll component that ships with Adobe Reader and Acrobat 9.x for Windows, Macintosh and UNIX operating systems. This vulnerability could cause a crash and potentially allow an attacker to take control of the affected system.

72. Zeus

Zeus also known as Zbot is a Trojan horse. It is the biggest and the most dangerous banking Trojan. These nastiest pieces of malware act as a money-stealing machine that steals banking information. Zeus is spread mainly from a drive-by download from a malicious website or via a phishing email which directs you to a fake or spoof website.

Zeus has also been tied to social media. Sometimes this infection is hidden in a false LinkedIn connection requests and lurking in some Facebook friend requests; if you accept a stranger and are suddenly asked to download a new version of flash it is a Trojan.

It was first identified in July 2007 when it was used to steal information from the United States Department of Transportation; it became more widespread in March 2009.

Once a Zeus Trojan infects a machine, it remains dormant until the end user visits a Web page with a form to fill out. One of the most powerful features is that it allows criminals to add fields to forms at the browser level. This means that instead of directing the end user to a counterfeit website, the user would see the legitimate website but might be asked to fill in an additional blank with specific information for "security reasons."

The Zeus Trojan can lay dormant for long periods until the user of the infected machine accesses targeted information, like banking accounts. Zeus then harvests passwords and authentication codes.

Illustration:

March 2010: Cyber Fraud Defendant was Charged and Sentenced in Manhattan Federal Court. The investigation targeted Global Bank Fraud Scheme that Used Zeus Trojan and Other Malware to Steal Millions of Dollars from U.S. Bank Accounts.

Illustration:

NIKOLAY GARIFULIN was sentenced in Manhattan federal court to two years in prison for his involvement in a global bank fraud scheme that used hundreds of phony bank accounts to steal over $3 million from dozens of U.S. accounts that were compromised by malware attacks.

Illustration:

As part of the bank fraud scheme, hackers in Eastern Europe used cyber attacks to steal money from the bank accounts of small and mid-sized businesses throughout the United States. The cyber attacks included the use of malware known as Zeus Trojan, which would embed itself in victims' computers and record their keystrokes as they logged into their online bank accounts. The hackers responsible for the malware then used the account information to take over the victims' bank accounts and make unauthorized transfers of thousands of dollars at a time to accounts controlled by co-conspirators

73. Zombie

In computer science, a zombie is a computer connected to the Internet that has been compromised by a hacker who secretly infiltrates an unsuspecting victim's computer so as to cause mischief or harm to him. The user generally remains unaware that his computer has been taken over since he can still use it, although it might slow down considerably.

Zombies have been used extensively to send e-mail spam; as of 2005, an estimated 50–80% of all spam worldwide was sent by zombie computers. They are also used to commit click fraud against sites and pay per click advertising, while others host phishing or money mule recruiting websites.

Distributed denial-of-service attack is another example of appliance of zombie computers overtaken by hackers to perform criminal activities.

One can look out for the following warning signs to check a Zombie Computer:

- You may receive emails accusing you of sending spam
- You may find email messages in your “outbox” that you didn’t send
- Your computer may start using more power than it has in the past to run the programs you use. Making the system slower.